高等学校教材

抽象代数基础

丘维声　编著



高等教育出版社







定价 11.80 元

抽象代数基础

丘维声　编著

高等教育出版社

图书在版编目(CIP)数据

抽象代数基础/丘维声编著.—北京:高等教育出版社,2003.8

ISBN 7-04-011873-4

Ⅰ.抽… Ⅱ.丘… Ⅲ.抽象代数-高等学校-教材 Ⅳ.0153

中国版本图书馆CIP数据核字(2003)第052460号

出版发行	高等教育出版社	购书热线	010-64054588
社　　址	北京市西城区德外大街4号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-82028899		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	北京地质印刷厂		
开　　本	850×1168　1/32	版　　次	2003年8月第1版
印　　张	7.625	印　　次	2003年8月第1次印刷
字　　数	200 000	定　　价	11.80元

内容简介

本书是大学数学系必修课“抽象代数”(或“近世代数”)课程的教材.全书分三章:第一章群,包括群的典型例子、子群和陪集、群的同构、群的直积、群的同态、正规子群、商群、群在集合上的作用、Sylow 定理、有限 abel 群的结构、自由群等;第二章环,包括理想、商环、环的同态、环的直和、素理想和极大理想、有限域的构造、唯一因子分解整环、主理想整环、欧几里得整环、Galois 环的构造、分式域等;第三章域扩张及其自同构,包括分裂域、有限域的结构、域扩张的自同构、伽罗瓦群、伽罗瓦扩张、本原元素、迹与范数等.本书按节配置习题,书末附有习题的提示或答案.

本书根据信息时代的需要精选内容,抓住主线;重视实例和应用,整合知识点;通俗易懂,讲清楚背景和想法;全盘考虑高等代数课和抽象代数课的教学内容,使之成为一个有机整体;注重培养学生科学的思维方式.

本书可作为综合大学、理工科大学和师范院校数学系的抽象代数(或近世代数)课程的教材,也可作为数学工作者和科技工作者进行科研工作的参考书,还可供学过高等代数课程的读者自学.

郑重声明

策划编辑　李　蕊

责任编辑　胡乃炯

封面设计　于　涛

责任绘图　黄建英

责任印制　宋克学

前　　言

抽象代数是现代数学的一个重要分支，它主要研究各种代数结构(即，具有代数运算的集合)，以及在这些结构中保持运算的映射(称为态射)．抽象代数为现代数学、现代物理学、现代化学、计算机科学、现代通信、以及密码学等提供了语言、重要结论和研究方法．当今信息时代，抽象代数有了越来越多的重要应用．抽象代数课程已经成为大学数学系的主干基础课之一．如何教好这门课程？作者根据自己80年代以来在北京大学数学系讲授抽象代数课的体会，把2002年秋季学期给数学科学学院210名学生讲授抽象代数课的讲稿整理成本书，并着重在以下几方面做了一些尝试．

精选内容，抓住主线．我们从信息时代的要求出发，精选抽象代数课程的教学内容．着重讲那些最基本和应用最广泛的内容，讲那些有信息时代气息的内容．全书分成三章：第一章群，第二章环，第三章域扩张及其自同构，对于每一章的内容都抓住主线：第一章的主线是群同态，第二章的主线是理想，第三章的主线是域扩张及其自同构．

重视实例和应用，整合知识点．我们在引言中，从如何度量对称性引出了群的概念，指出群可以用来度量对称性，群可以用来分类几何学，群可以用来判定代数方程能否用根式求解．接着在第一章§1，我们讲了群的典型例子，包括来自数集、几何、代数中群的例子，从中介绍了循环群、二面体群，矩阵群，对称群和交错群等．这使我们在以后各节里可以充分运用这些实例来帮助理解抽象的概念和结论．我们不停留在让学生知道概念的定义上，而且阐述概念的应用．例如在第一章§3，我们从比较二次单位根群 U_2 的乘法表与模2剩余类环 $\mathbf{Z}_2$ 的加法群的加法表，引出了群的同构的概念之后，接着证明了任一无限循环群都与整数加群 $\mathbf{Z}$ 同构，任意一个 m 阶循环群都与 $\mathbf{Z}_m$

的加法群同构.我们在这一节还决定了4阶群的同构类,并且为了找出一个比较简单的4阶非循环的abel群,我们引出了群的直积的概念,还证明了$\mathbf{Z}_m \times \mathbf{Z}_n$是循环群当且仅当$(m,n)=1$,从而可以识别$\mathbf{Z}_m \times \mathbf{Z}_n$是否同构于$\mathbf{Z}_{mn}$.又如在第二章§3,我们讲了极大理想的概念及其充分必要条件之后,接着讲有限域的构造.进而在§4,我们又讲了代数数域和Galois环的构造.在整本书中,我们从理论的应用的角度,以及内容之间的内在联系的角度,整合了各知识点,把第一章的内容整合成8节,第二章的内容整合成6节,第三章的内容整合成了3节,详见目录.

通俗易懂,讲清楚背景和想法.我们对于重要的概念都要先讲这个概念产生的背景.例如,在第一章§4,我们从茶杯的三视图能反映茶杯的形状这一通俗例子出发,引出了群的同态的概念.在第二章§1,我们从xOy平面上的单位圆C可看成是圆柱面$x^2+y^2-1=0$与xOy平面$z=0$的交,又可看成是单位球面$x^2+y^2+z^2-1=0$与圆柱面$x^2+y^2-1=0$的交等等,引出其零点集包含C的所有3元实系数多项式组成的集合I,并且分析I的性质:对减法封闭、有"吸收性",由此引出理想的概念.我们对于重要的定理,先通过具体例子,猜出可能有的结论,然后进行论证.在论证中特别注意讲清楚关键想法,而且还讲清楚这个关键想法产生的背景,即这个关键想法是怎么想出来的.例如在第一章§7,我们先让学生观察4阶群,9阶群,8阶abel群有多少种互不同构的类型,看出这些abel群都同构于循环群或者若干个循环群的直积,然后问:任意有限abel群是否也有这样的结构?根据Sylow第一定理容易把这个问题归结为研究abel p-群的结构.在证明abel p-群的结构定理之前,我们讲了两个关键想法,并且讲了这两个关键想法是怎么想出来的,然后才讲证明.

全盘考虑高等代数(Ⅰ)、(Ⅱ)和抽象代数课程的教学内容,使之成为一个有机整体.高等代数(Ⅰ)、(Ⅱ)和抽象代数是大学数学系在

代数方面的必修课，共三个学期．作者在去年下半年给数学科学学院本科生讲授抽象代数课时，对于抽象代数课与高等代数（Ⅰ）、（Ⅱ）的教学内容作了统筹安排，对作者编写的《高等代数（上册、下册）》进行了修订，同时详细写了抽象代数每一次大课的讲稿．大体上说，高等代数（Ⅰ）讲授线性代数的具体部分，内容包括：线性方程组、行列式、数域 K 上 n 元有序数组的向量空间 K^n、矩阵的运算、K^n 到 K^s 的线性映射（即 $\mathbf{A}\alpha = A\alpha$）、欧几里得空间 $\mathbf{R}^n$、矩阵的相抵分类、矩阵的相似以及矩阵的特征值和特征向量、二次型与矩阵的合同．高等代数（Ⅱ）讲授多项式环（着重讲一元多项式环的理论），介绍模 m 剩余类环 $\mathbf{Z}_m$ 和模 p 剩余类域 $\mathbf{Z}_p$，以及域的特征；讲授线性代数的抽象部分，内容包括：域上的线性空间、线性映射（包括线性变换和线性函数）、具有度量的线性空间（包括欧几里得空间、酉空间、以及正交空间和辛空间简介）．抽象代数讲授群的结构、环的结构、域扩张及其自同构．我们努力使这三个学期的代数课程成为一个有机整体．例如，我们在《高等代数（第二版）下册》的第七章 §8 详细讨论了 $\mathbf{Q}[x]$ 中本原多项式的性质，证明了每一个次数大于 0 的本原多项式可以唯一地分解成 $\mathbf{Q}$ 上不可约的本原多项式的乘积．这样我们在本书的第二章 §6 中，利用上述结论很容易地得出，$\mathbf{Z}[x]$ 中每一个次数大于 0 的本原多项式可以唯一地分解成 $\mathbf{Z}$ 上不可约的本原多项式的乘积，进而证明了 $\mathbf{Z}[x]$ 是唯一因子分解整环，即高斯整环．接着我们指出，上述证明 $\mathbf{Z}[x]$ 是高斯整环的方法也可用于证明下述结论：高斯整环 R 上的一元多项式环 $R[x]$ 也是高斯整环．这样不仅节省了教学时间，而且使高等代数课与抽象代数课的教学内容前后呼应，有利于学生对抽象理论的理解．

注重培养学生科学的思维方式．我们认为讲授一门课程不仅要让学生掌握本门课程的基本知识、基本方法，受到本门课程的基本训练，而且要培养学生具有科学的思维方式．数学的思维方式就是一种科学的思维方式．我们把数学的思维方式概括为：观察客观现象，抓

住其主要特征,抽象出概念或者建立模型;进行探索,通过直觉判断或者归纳推理、类比推理以及联想等作出猜测;然后进行深入分析和逻辑推理以及计算,揭示事物的内在规律,从而使纷繁复杂的现象变得井然有序.这就是数学思维方式的全过程.我们按照数学思维方式讲课,可以使学生从中受到熏陶,既使他们比较顺利地学好目前的课程,又有助于他们把今后肩负的工作做好.

本书的每一节都配备了习题,书末附有习题的提示或答案.

本书可作为综合大学、理工科大学和师范院校的数学系抽象代数(或近世代数)课程的教材.书中加"*"号的内容和用楷体字排印的内容不作为教学要求,供有兴趣的读者自己看.

作者感谢本书的责任编辑胡乃冏编审,他为本书的编辑出版付出了辛勤的劳动.

作者热忱地欢迎广大读者对本书提出宝贵意见.

丘维声

于北京大学 数学科学学院

2003年5月

目　录

引言 …………………………………………………………………… (1)

第一章　群 ……………………………………………………… (11)

§1　群的典型例子：循环群，二面体群，矩阵群，对称群 ……………………………………………………… (11)

§2　子群，陪集，Lagrange 定理，循环群的子群 ………… (25)

§3　群的同构，群的直积 ………………………………… (40)

§4　群的同态，正规子群，商群，可解群 ………………… (50)

§5　群在集合上的作用，群的自同构，轨道—稳定子定理 ……………………………………………………… (66)

§6　Sylow 定理 ……………………………………………… (82)

§7　有限 abel 群的结构 ………………………………… (92)

§8　自由群，群的表现 …………………………………… (102)

第二章　环 ……………………………………………………… (114)

§1　环的类型和性质，理想 ……………………………… (114)

§2　商环，环的同态，环的直和 ………………………… (123)

§3　素理想和极大理想，有限域的构造 ………………… (134)

§4　代数数域和 Galois 环的构造 ……………………… (143)

*§5　分式域 ………………………………………………… (152)

§6　唯一因子分解整环，主理想整环，欧几里得整环 … (156)

第三章　域扩张及其自同构 …………………………………… (171)

§1　域扩张，分裂域，有限域的结构，正规扩张 ………… (171)

§2　域扩张的自同构，伽罗瓦群，伽罗瓦扩张 ………… (185)

§3 本原元素、迹与范数……………………………… (195)
习题的提示或答案 ……………………………… (200)
参考文献 ……………………………… (228)
索引 ……………………………… (229)

引　言

一、抽象代数的研究对象

自然界和现实生活中，美丽的蝴蝶，多姿的雪花，绚丽的墙纸，耀眼的窗花，……无不具有对称性，而使人心旷神怡.

如何度量对称性(symmetry)?

例如，我们很容易看出，等边三角形比等腰三角形(它的腰与底不相等)更具有对称性，道理是什么呢？

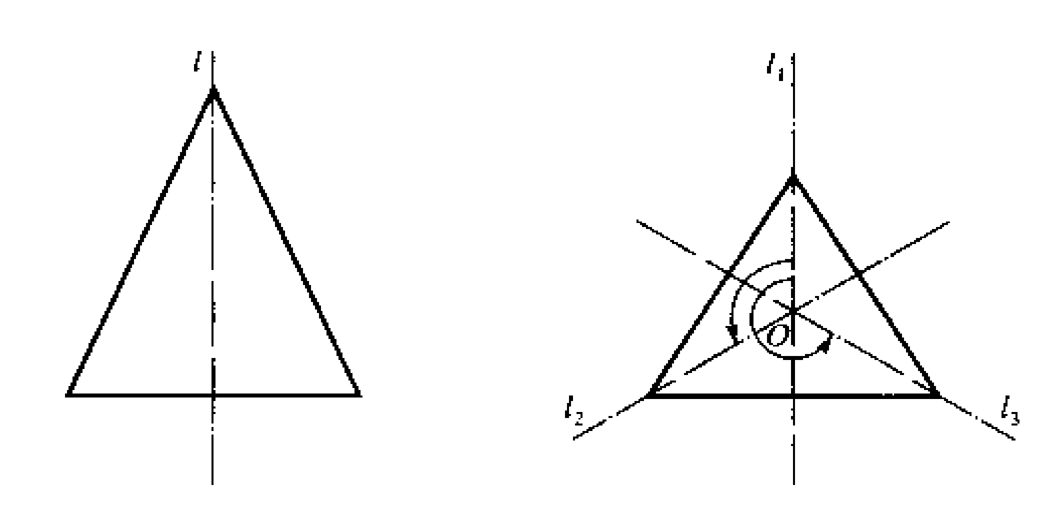


图 0-1

设等腰三角形底边上的垂直平分线为 l，则平面上关于 l 的反射 τ 把等腰三角形变成与它自己重合的图形. 显然，平面的恒等变换 I 也具有这个性质.

设等边三角形(equilateral triangle)的中心为 O，三条边上的垂

直平分线分别为 l_1, l_2, l_3. 则平面上关于 l_i 的反射 τ_i 把等边三角形变成与它自己重合的图形, $i=1,2,3$; 平面上绕点 O 的转角分别为 $\frac{2\pi}{3}, \frac{4\pi}{3}$ 的旋转 σ_1, σ_2, 以及恒等变换 I 也具有这个性质.

平面上(或空间中)的正交(点)变换(也称保距变换(isometry)), 如果把平面(或空间)图形 Γ 变成与它自己重合的图形, 则把这个正交(点)变换叫做图形 Γ 的**对称(性)变换**.

上面指出, 等边三角形的对称(性)变换已经有6个. 进一步可以证明, 只有这 6 个. 类似地, 等腰三角形(它的腰与底不相等)的对称(性)变换有且只有两个. 我们自然可以说: 等边三角形比等腰三角形更具有对称性.

我们把等边三角形的所有对称(性)变换组成一个集合:

$$G = \{I, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}.$$

我们知道, 平面上两个正交(点)变换的乘积仍是正交(点)变换; 并且如果它们都把等边三角形变成与它自己重合的图形, 那么它们的乘积也有这个性质. 因此等边三角形的任意两个对称(性)变换的乘积仍是它的对称(性)变换. 从而集合 G 对于映射的乘法封闭. 因此映射的乘法是集合 G 上的一个(二元)代数运算.

一般地, 非空集合 S 与自己的笛卡儿积 $S \times S$ 到 S 的一个映射, 称为 S 上的一个**二元代数运算**, 简称为 S 上的代数运算.

由于映射的乘法适合结合律, 因此上述集合 G 上的代数运算适合结合律.

G 中有恒等变换 I, I 与 G 中任一元素的乘积(左乘或右乘)都等于那个元素自己.

容易看出, G 中每个变换都有逆变换. 例如, $\sigma_1^{-1} = \sigma_2, \tau_i^{-1} = \tau_i$, $i = 1,2,3$.

从上面的例子以及大量类似的例子, 我们抽象出下述概念:

定义 1 设 G 是一个非空集合, 如果在 G 上定义了一个代数运

算，通常称为乘法，记作 ab，并且它适合下列条件：

(i) 对于 G 中任意元素 a, b, c，有

$$(ab)c = a(bc) \text{（结合律）}; \tag{1}$$

(ii) G 中有一个元素 e，使得

$$ea = ae = a, \ \forall a \in G; \tag{2}$$

(iii) 对于 G 中任一元素 a，都有 G 中一个元素 b，使得

$$ab = ba = e, \tag{3}$$

那么 G 称为一个群(group).

容易说明，G 中满足(2)式的元素 e 是唯一的，称 e 是群 G 的**单位元素**(identity element)；对于 G 中元素 a，G 中满足(3)式的元素 b 是唯一的，称 b 是 a 的**逆元素**(inverse)，记作 a^{-1}. 于是(3)式可以写成

$$aa^{-1} = a^{-1}a = e. \tag{4}$$

从(4)式看出，a^{-1} 的逆元素是 a，即 $(a^{-1})^{-1} = a$.

群 G 的运算也可以称为加法，记作 $a + b$，此时结合律为

$$(a + b) + c = a + (b + c), \quad \forall a, b, c \in G;$$

单位元素称为零元素，记成 0；a 的逆元素称为 a 的负元素，记成 $-a$.

如果群 G 的运算还适合交换律，即对任于 G 中任意元素 a、b，有 $ab = ba$，则称 G 为**交换群(或 abel 群)**.

从上面的讨论知道，等边三角形的所有对称(性)变换组成的集合 G，对于映射的乘法成为一个群. 用类似的方法可以说明：

图形 Γ 的所有对称(性)变换组成的集合 G，对于映射的乘法成为一个群，称 G 是**图形 Γ 的对称(性)群**(symmetry group).

上述表明，群可以用来度量对称性.

用群来度量对称性的重要意义在于：我们可以通过研究群的分类，来对具有对称性的客观事物进行分类.

例如，现实生活中，常常用正方形或正六边形的砖铺地板，如图 0－2；也常常用具有对称性图案的纸贴墙壁，如图 0－3.

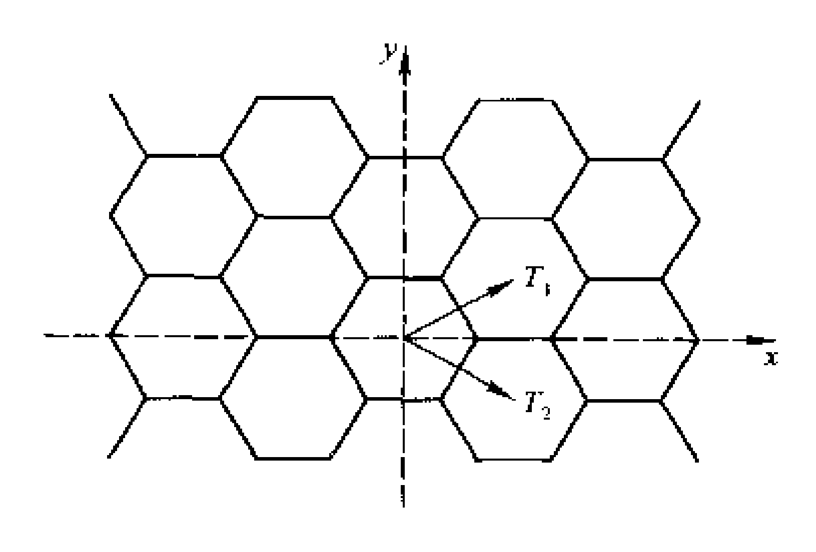


图 0－2

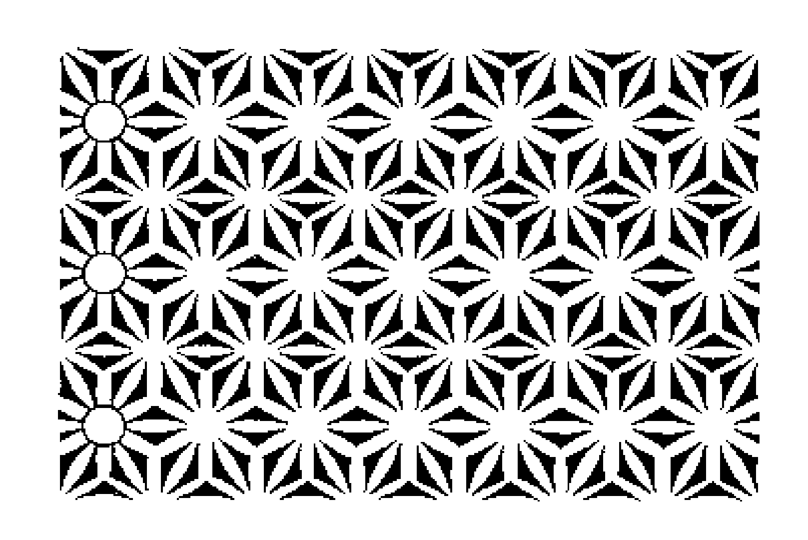


图 0－3

设想这些图案分别铺满了整个平面.如果铺满了图案的平面的对称(性)群不固定一个点,也不固定一条直线,则称它为**平面晶体群**(plane crystallographic group)(或者称为**贴墙纸群**(wallpaper group)). R.Fricke 和 F.Klein 在他们关于自同构函数的第一本书(1897)中,对平面晶体群进行分类.G.Polya 在1924年表的一篇文章中,完成了对平面晶体群的分类:共有 17 种不同的平面晶体群,并且

给出了相应的装饰图案式样的例子.

自然界中有各种各样的晶体,每一种晶体的原子结构的模型可以看成是空间中的点阵.设想将这种点阵连续地、无限地填充整个空间.填充了点阵的空间的对称(性)群,如果既不固定一个点,也不固定一条直线,而且不固定一个平面,则称它为**空间晶体群**(space crystallographic group).对空间晶体群进行分类,就可以了解自然界中各种晶体的结构.在1868年,C. Jordan借助Bravais(1848)对晶体结构分类的工作,研究空间晶体群的分类,虽然没有完全分类,但是这为E. S. Fedorov(1890)和A. Schönflies(1891)的工作铺平了道路.Fedorov和Schönflies分别独立地证明了空间晶体群共有230个.这是历史上将群论直接用于自然科学的第一个例子.Fricke和Klein在他们的书(1897)中对平面晶体群的分类,就是受到Fedorov和Schönflies的工作的激励.Polya在1924年发表的文章中,感谢Schönflies的书对他的促进.

欧几里得几何的第五公设(也称平行公设),它的叙述不像其它4条公设那样简洁、明了.因此从古希腊时代开始,数学家们就一直没有放弃消除对第五公设疑问的努力,高斯(Gauss)从1799年开始意识到平行公设不能从其他的欧几里得公理推出来,并从1813年起发展了这种平行公设在其中不成立的新几何,称为"非欧几里得几何".罗巴切夫斯基(Н. И. Лобачевский)从1826年开始,报告了自己关于非欧几何的发现.黎曼(B. Riemann)在1854年发展了罗巴切夫斯基等人的思想而建立了一种更广泛的几何,即现在所称的黎曼几何,罗巴切夫斯基的非欧几何和通常的欧几里得几何是黎曼几何中的两种特殊情形.非欧几何揭示了空间的弯曲性质,将平直空间的欧氏几何变成了某种特例.而射影几何的发展,又从另一个方向使欧氏几何成为特例.

19世纪的几何学园地朵朵鲜花竞相开放.在这样的形势下,寻找不同几何学之间的内在联系,用统一的观点来解释它们,便成为数

学家们追求的一个目标，统一几何学的第一个大胆计划是由德国数学家克莱因(F. Klein)提出的. 1872 年，克莱因被聘为爱尔朗根大学的数学教授. 他在就职演讲中阐述了几何学统一的思想：所谓几何学，就是研究几何图形对于某类变换群保持不变的性质的学问，或者说任何一种几何学只是研究与特定的变换群有关的不变量. 他的这次演讲被称为《爱尔朗根纲领(Erlangen Program)》. 欧几里得几何就是研究图形在正交(点)变换群下保持不变的性质，而研究图形在仿射变换群下保持不变的性质的几何，称为仿射几何；研究图形在射影变换群下保持不变的性质的几何，称为射影几何.(关于正交(点)变换，仿射变换，射影变换的概念可以参看《解析几何(第二版)》，丘维声编，北京大学出版社 1996 年出版).

上述表明，群可以用来分类几何学.

二次方程的解法古巴比伦人就已掌握，16 世纪由 S. Ferro, N. Fontana, G. Cardano, L. Ferrari 先后给出了三次、四次方程的根式解. 此后人们便着力研究高次方程(即，五次和五次以上的方程)的根式解问题. 到了 18 世纪，拉格朗日(J. L. Lagrange)在 1770 年发表长篇论文《关于代数方程解的思考》. 他在其中探讨一般三、四次方程能用根式求解的原因. 在 1799 年，鲁菲尼(P. Ruffini)明确提出要证明高于四次的一般方程不可能用代数方法求解. 到了 19 世纪，阿贝尔(N. H. Abel)在 1824 年自费出版了一本小册子《论代数方程，证明一般五次方程的不可解性》，在其中严格证明了以下事实：如果方程的次数 $n \geqslant 5$，并且系数 $a_1, a_2, \cdots, a_n$ 看成是字母，那么任何一个由这些字母组成的根式都不可能是方程

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0 \tag{5}$$

的根. 这样，五次和高于五次的一般方程不能用根式求解的问题就由阿贝尔解决了. 在阿贝尔的工作之后，数学家所面临的一个问题是：什么样的特殊方程能够用根式求解？这个问题被伽罗瓦(E. Galois)解决，伽罗瓦在 1829—1831 年间完成的几篇论文中，建立了判别代

数方程可用根式求解的充分必要条件,从而宣告了代数方程用根式求解这一经历了三百年的难题的彻底解决.伽罗瓦的思想是将 n 次方程(5)的 n 个根 $x_1,x_2,\cdots,x_n$ 作为一个整体来考察,令 $\Omega=\{x_1,x_2,\cdots,x_n\}$,$\Omega$ 上的所有置换(Ω 到自身的双射称为置换)组成的集合 S_n 有一个代数运算:置换的乘法(即,映射的乘法).伽罗瓦称 S_n 为"群".这是历史上最早的"群"的定义,不过它只是针对一个具体的群(置换群)所作的定义,还不是抽象群的一般定义.伽罗瓦进一步考虑 S_n 中某些置换组成的"子群",伽罗瓦称之为"方程的群",也就是我们今天所说的"伽罗瓦群".方程的群刻画了方程的根的对称性.伽罗瓦证明了:方程 $f(x)=0$ 可用根式求解当且仅当方程的群是可解群.

伽罗瓦引进"群"的概念,导致了代数学在对象、内容和方法上的深刻变革.代数学不再仅仅是研究代数方程,而更多地是研究各种抽象的"对象"的运算关系,代数学的这些新的研究对象在现代数学、现代物理、现代化学以及通信科学、信息安全等现代社会生活领域中,都有重要应用.

从整数集 $\mathbf{Z}$,数域 K 上所有一元多项式组成的集合 $K[x]$,数域 K 上所有 n 级矩阵组成的集合 $M_n(K)$,模 m 剩余类组成的集合等抽象出环的概念.

定义 2　设 R 是一个非空集合,如果在 R 上定义了两个代数运算,一个叫加法,记为 $a+b$;另一个叫乘法,记为 ab,并且它们适合下列条件:

(i) R 对于加法成一个交换群;

(ii) 乘法的结合律:对 R 中任意元素 a,b,c,有

$$(ab)c=a(bc);$$

(iii) 乘法对加法的分配律:对所有的 $a,b,c\in R$,有

$$a(b+c)=ab+ac,\qquad(\text{左分配律}),$$

$$(b+c)a=ba+ca,\qquad(\text{右分配律}),$$

那么 R 称为一个环(ring).

如果环 R 的乘法还适合交换律,则称 R 为**交换环**(commutative ring).

如果环 R 中有一个元素 e 具有性质:对于 R 中任意元素 a,有 $ae = ea = a$,则称 e 是 R 的**单位元素**,称 R 是有单位元的环,通常把 R 的单位元就记成 1.

在有单位元的环 R 中,对于元素 a,如果 R 中有元素 b,使得 $ab = ba = 1$,则称 a 是**可逆元**(invertible element)(或**单位**(unit)),此时把 b 称为 a 的**逆元**,记成 a^{-1}.(注:可以说明,如果 a 是可逆元,则满足 $ab = ba = 1$ 的元素 b 是唯一的.)

定义 3　如果 F 是一个有单位元 $1(\neq 0)$ 的交换环,并且它的每一个非零元都可逆,则称 F 是一个**域**(field).

从域的定义看出,域 F 有两个代数运算:加法和乘法,并且 F 对于加法成一个交换群,F 的所有非零元组成的集合 F^* 对于乘法也成一个交换群,并且适合乘法对于加法的分配律.

有理数域 $\mathbf{Q}$,实数域 $\mathbf{R}$,复数域 $\mathbf{C}$ 等数域都是域.

可以证明:当 p 为素数时,模 p 剩余类环 $\mathbf{Z}_p$ 是一个域(证明参看《高等代数(下册)》,丘维声编著,高等教育出版社,1996 年出版,第 150 页).称 $\mathbf{Z}_p$ 是模 p 剩余类域.一个域如果只有有限个元素,则称它为**有限域**.

有限域在现代通信和信息安全中有重要应用.

像群、环、域那样,具有代数运算的集合称为**代数结构**(algebraic structures).

抽象代数(abstract algebra)的研究对象是代数结构,并且是通过研究保持运算的映射(称为**态射**(morphism))来研究代数结构.

抽象代数使代数结构和态射成为代数学研究的中心.

二、抽象代数的重要性

抽象代数为现代数学、现代物理学、现代化学以及计算机科学、现代通信和密码学等提供了语言.

抽象代数研究结构和态射的思想已经渗透到现代数学的各个分支中.在很多数学对象的研究中都要首先建立适当的代数结构或其他结构,然后通过研究态射来研究这些结构.

抽象代数的研究方法和重要结论在现代数学的各个分支,以及现代物理学、计算机科学、通信科学、信息安全、经济学等等领域都有重要应用.

学习抽象代数可以受到数学思维方式的很好的训练,从而在培养科学的思维方式上有质的提高.

三、抽象代数的学习方法

1. 要按照数学的思维方式来学习抽象代数.

什么是数学的思维方式?观察客观世界的现象,抓住其主要特征,抽象出概念或者建立模型;进行探索,通过直觉判断或者归纳推理,类比推理以及联想等作出猜测;然后进行深入分析和逻辑推理以及计算,揭示事物的内在规律,从而使纷繁复杂的现象变得井然有序.这就是数学的思维方式.

2. 要多用具体例子来理解抽象代数的概念和结论.

3. 要抓住抽象代数研究代数结构,并且通过研究态射来研究代数结构这条主线.

4. 要在理解的基础上记住基本概念和重要结论.

5. 要运用抽象代数的研究方法和重要结论去解决具体问题.

6. 要做一定数量的习题,才能理解概念,掌握理论和提高分析

问题的能力.

习　题

1. 证明:在群 G 中,对于任意元素 a,b,方程 $ax = b$ 有唯一解;方程 $ya = b$ 也有唯一解.

2. 证明:在群 G 中,消去律成立.即

由 $ax = ay$ 可以推出 $x = y$;

由 $xa = ya$ 可以推出 $x = y$.

3. 模 4 剩余类环 $\mathbf{Z}_4$ 中,所有非零元组成的集合 $\mathbf{Z}_4^*$ 对于乘法是否成为一个群?

4. 求出 $\mathbf{Z}_8$ 中的所有可逆元.

*5. 证明:在模 m 剩余类环 $\mathbf{Z}_m$ 中,a 可逆当且仅当 $(a, m) = 1$.

第一章　群

§1　群的典型例子:循环群,二面体群,矩阵群,对称群

一个群是指一个非空集合 G,它满足下列 4 个条件:

(i) 在 G 上定义了一个(二元)代数运算;

(ii) G 上的运算适合结合律;

(iii) G 中有一个元素 e,具有下述性质:

$$ae = ea = a, \quad \forall a \in G,$$

称 e 是 G 的单位元素;

(iv) G 中每一个元素都有逆元.

如果 G 满足条件(i)、(ii),则称 G 为**半群**(semigroup);如果 G 满足条件(i)、(ii)、(iii),则称 G 为**幺半群**(monoid).

群 G 中不同元素的逆元是不同的.这是因为如果 G 中,$a^{-1}=b^{-1}$,则 $(a^{-1})^{-1}=(b^{-1})^{-1}$,从而 $a=b$.

容易验证,群 G 中,有

$$(ab)^{-1}=b^{-1}a^{-1}. \tag{1}$$

由于群 G 的运算适合结合律,因此 n 个元素 $a_1,a_2,\cdots,a_n$ 的乘积是唯一确定的,把它记作 $a_1a_2\cdots a_n$.容易验证:

$$(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}. \tag{2}$$

群 G 中,n 个 a 的乘积记作 a^n,读作"a 的 n 次幂".即

$$a^n \xlongequal{\text{def}} \underbrace{a\cdot a\cdots a}_{n个}, \quad n\in \mathbf{Z}^+. \tag{3}$$

我们还规定：

$$a^0 \overset{\text{def}}{=\!=} e, \tag{4}$$

$$a^{-n} \overset{\text{def}}{=\!=} (a^{-1})^n, \quad n \in \mathbf{Z}^+. \tag{5}$$

容易验证：

$$a^n a^m = a^{n+m}, \quad n,m \in \mathbf{Z}; \tag{6}$$

$$(a^n)^m = a^{nm}, \quad n,m \in \mathbf{Z}. \tag{7}$$

注意，一般地 $(ab)^n \neq a^n b^n$，$n,m \in \mathbf{Z}$.

如果群 G 的运算写成加法，则把 a^n 写成 na，读作"a 的 n 倍". 此时把(3)—(7) 式分别写成

$$na \overset{\text{def}}{=\!=} \underbrace{a + a + \cdots + a}_{n\text{个}}, \quad n \in \mathbf{Z}^+, \tag{8}$$

$$0a \overset{\text{def}}{=\!=} 0, \tag{9}$$

$$(-n)a \overset{\text{def}}{=\!=} n(-a), \quad n \in \mathbf{Z}^+; \tag{10}$$

$$na + ma = (n+m)a, \quad n,m \in \mathbf{Z}, \tag{11}$$

$$m(na) = (mn)a, \quad m,n \in \mathbf{Z}. \tag{12}$$

注意(9) 式中等号左边"$0a$"中的 0 是整数，而右边的 0 是群 G 中的单位元素(也称零元).

如果群 G 有无限多个元素，则称 G 为**无限群**.

如果群 G 只有有限多个元素，则称 G 为**有限群**. 此时，G 中元素的个数称为 G 的**阶**(order)，记作 $|G|$.

(一) 来自数集中群的例子

例 1 整数集 $\mathbf{Z}$ 对于加法成为一个群，通常称它为**整数加群**.

思考：所有非零整数组成的集合 $\mathbf{Z}^*$ 对于乘法是否成一个群？

例 2 实数集 $\mathbf{R}$ 对于加法成一个群，通常称它为**实数加群**.

思考：非零实数集 $\mathbf{R}^*$ 对于乘法是否成一个群？

例 3 正实数集 $\mathbf{R}^+$ 对于乘法成一个群.

例 4 在复数集 $\mathbf{C}$ 中，对于给定的正整数 n，所有 n 次单位根（即 $z^n=1$ 的根）组成的集合，对于复数乘法成一个群，称它为 **n 次单位根群**，记作 U_n. 例如，二次单位根群 $U_2=\{1,-1\}$；四次单位根群 $U_4=\{1,-1,i,-i\}$，其中 i 是虚数单位.

观察例 1 和例 4 中的群在结构上有什么共同点.

例 1 的整数加群 $\mathbf{Z}$ 中，利用公式(8)、(9)、(10)，每一个整数 k 可以写成 1 的 k 倍，即 $k=k1$，很自然地把 1 叫做整数加群 $\mathbf{Z}$ 的**生成元**. 此时整数加群 $\mathbf{Z}$ 可以写成

$$\mathbf{Z}=\{k1 \mid k\in\mathbf{Z}\}, \tag{13}$$

还可以更简洁地写成

$$\mathbf{Z}=\langle 1\rangle. \tag{14}$$

例 4 的 n 次单位根群 U_n 中，所有 n 次单位根为 $e^{i\frac{2k\pi}{n}}$，$k=0,1,\cdots,n-1$. 令 $\xi=e^{i\frac{2\pi}{n}}$，则每一个 n 次单位根可以写成 ξ^k，从而

$$U_n=\{\xi^k \mid k=0,1,\cdots,n-1\}. \tag{15}$$

很自然地把 ξ 叫做 U_n 的**生成元**. 此时 U_n 可以写成

$$U_n=\langle\xi\rangle. \tag{16}$$

像整数加群 $\mathbf{Z}$，n 次单位根群 U_n 这样，如果群 G 的每一个元素都能写成 G 中某一个元素 a 的方幂（G 的运算记成乘法）或者倍"数"（G 的运算记成加法），则称 G 为**循环群**(cyclic group)，把 a 叫做 G 的**生成元**(generator). 此时可以把 G 记成 $\langle a\rangle$.

思考：循环群 G 的生成元是唯一的吗？试调查整数加群 $\mathbf{Z}$ 的生成元，以及 n 次单位根群 U_n 的生成元.

U_n 的生成元称为复数域中的**本原 n 次单位根**. (primitive nth root of unity)

显然，整数加群 $\mathbf{Z}$ 是无限循环群；n 次单位根群 U_n 是有限循环群，U_n 的阶为 n. 显然，循环群是 abel 群.

(二) 来自几何中群的例子

例 5　平面(或空间)的所有正交点变换(也称保距变换)组成的集合，对于映射的乘法成一个群，称它为平面(或空间)欧几里得群，记作 E_2(或 E_3).

例 6　正方形的对称(性)群 G 的结构.

如图 1－1，正方形 $A_1A_2A_3A_4$ 的对称中心为 O，4 条对称轴分别记作 l_1,l_2,l_3,l_4.

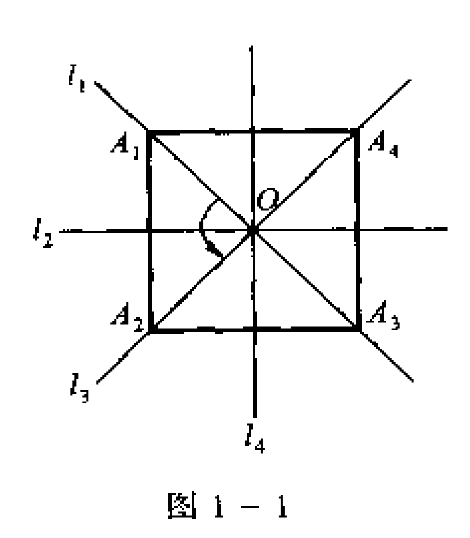


图 1－1

用 σ 表示绕点 O 转角为 $\frac{\pi}{2}$ 的旋转，则 σ^2,σ^3 分别表示绕点 O 转角为 $\pi,\frac{3\pi}{2}$ 的旋转.

用 τ_i 表示关于直线 l_i 的反射，$i=1,2,3,4$.

用 I 表示平面的恒等变换.

显然正方形 $A_1A_2A_3A_4$ 的对称(性)群 G 至少包含上述 8 个元素：$I,\sigma,\sigma^2,\sigma^3,\tau_1,\tau_2,\tau_3,\tau_4$. G 中还有其他元素吗?

任取 $\gamma\in G$，由于正方形的对称(性)变换把正方形的中心 O 保持不动，因此它或者是绕点 O 的旋转，或者是关于过 O 点的直线的反射，或者是它们的乘积. 图 1－1 中正方形顶点的有序组 $A_1A_2A_3A_4$ 成逆时针方向，绕点 O 的旋转使 $A_1A_2A_3A_4$ 仍成逆时针方向. 而关于过点

O 的直线的反射，或者旋转与反射的乘积，使 $A_1A_2A_3A_4$ 成顺时针方向. 现在设 γ 把顶点 A_1 变成 A_j，$j \in \{1,2,3,4\}$.

情形 1. γ 使 $A_1A_2A_3A_4$ 成逆时针方向，则 γ 必定是绕点 O 的旋转. 由于 γ 把 A_1 变成 A_j，因此转角为 $(j-1)\dfrac{\pi}{2}$. 从而 $\gamma = \sigma^{j-1}$.

情形 2. γ 使 $A_1A_2A_3A_4$ 成顺时针方向，则 $\gamma = \tau_j$ 或者 $\gamma = \sigma^{j-1}\tau_1$（这里 τ_1 使 $A_1A_2A_3A_4$ 成顺时针方向，σ^{j-1} 把 A_1 变成 A_j）. 容易验证 $\tau_j = \sigma^{j-1}\tau_1$.

由于 $j \in \{1,2,3,4\}$，因此

$$\gamma \in \{I, \sigma, \sigma^2, \sigma^3, \tau_1, \sigma\tau_1, \sigma^2\tau_1, \sigma^3\tau_1\}. \tag{17}$$

从而

$$G \subseteq \{I, \sigma, \sigma^2, \sigma^3, \tau_1, \sigma\tau_1, \sigma^2\tau_1, \sigma^3\tau_1\}. \tag{18}$$

于是 $|G| \leqslant 8$，又从前面知道，$|G| \geqslant 8$. 因此 $|G| = 8$. 从而

$$G = \{I, \sigma, \sigma^2, \sigma^3, \tau_1, \sigma\tau_1, \sigma^2\tau_1, \sigma^3\tau_1\}. \tag{19}$$

从(19)式，很自然地可以把 σ、τ_1 称为 G 的**生成元**. 它们具有性质：

$$\sigma^4 = I, \quad \tau_1^2 = I. \tag{20}$$

由于 $\sigma\tau_1 = \tau_2$，因此 $(\sigma\tau_1)^2 = \tau_2^2 = I$，即 $(\sigma\tau_1)(\sigma\tau_1) = I$. 由此得出

$$\tau_1\sigma\tau_1 = \sigma^{-1}. \tag{21}$$

由于 $\sigma\sigma^3 = \sigma^4 = I$，因此 $\sigma^{-1} = \sigma^3$. 于是 $\tau_1 \cdot \sigma\tau_1 = \sigma^3$. 有了公式(20)，(21)以后，$G$ 中任意两个元素的乘积就都可以计算出来了，我们把(20)，(21)式称为 G 的生成元适合的关系(relations). 这样我们就把正方形的对称(性)群 G 的结构完全搞清楚了：它有两个生成元，且适合关系(20)，(21). 我们可以把 G 简洁地写成

$$G = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = I,\ \tau\sigma\tau = \sigma^{-1} \rangle, \tag{22}$$

其中 $\tau = \tau_1$. 事实上 τ 可以是关于正方形的任意一条对称轴的反射.

上面对于正方形的对称(性)群的结构的研究方法，完全适用于任何一个正 n 边形($n \geqslant 3$). 因此可以得出下述结论：

设正 n 边形($n \geqslant 3$)的对称中心为 O，用 σ 表示绕点 O 转角为

$\frac{2\pi}{n}$的旋转；用 τ 表示关于某条对称轴的反射，则正 n 边形的对称(性)群 G 为

$$G = \{I, \sigma, \sigma^2, \cdots, \sigma^{n-1}, \tau, \sigma\tau, \cdots, \sigma^{n-1}\tau\}; \tag{23}$$

σ, τ 是 G 的两个生成元，G 还可以写成

$$G = \langle \sigma, \tau \mid \sigma^n = \tau^2 = I, \quad \tau\sigma\tau = \sigma^{-1} \rangle. \tag{24}$$

我们把正 n 边形的对称(性)群叫做**二面体群**(dihedral group)，记作 $D_n(n \geqslant 3)$. 显然 D_n 的阶为 $2n$. 由于 $\tau\sigma\tau = \sigma^{-1}$，因此 $\sigma\tau = \tau^{-1}\sigma^{-1} = \tau\sigma^{n-1} \neq \tau\sigma$. 这说明 D_n 是非交换群.

(三) 来自代数中群的例子

例 7 模 m 剩余类环 $\mathbf{Z}_m$ 对于加法成一个循环群，它的生成元是 $\bar{1}$(因为 $\bar{i} = i\bar{1}$). $\mathbf{Z}_m$ 中所有可逆元组成的集合对于乘法成一个 abel 群，称它为 $\mathbf{Z}_m$ 的**单位群**(group of units)，记作 $U(\mathbf{Z}_m)$ 或者 $\mathbf{Z}_m^*$(这时不要与 $\mathbf{Z}_m$ 的所有非零元组成的集合 $\mathbf{Z}_m^*$ 混淆，这可从上下文看出 $\mathbf{Z}_m^*$ 到底表示什么).

特别地，当 p 为素数时，$\mathbf{Z}_p$ 为域. 此时 $\mathbf{Z}_p$ 的所有非零元组成的集合 $\mathbf{Z}_p^*$ 对于乘法成一个 abel 群，称它为 $\mathbf{Z}_p$ 的乘法群.

例 8 域 F 上的线性空间 V，对于加法成一个 abel 群.

例 9 域 F 上所有 n 级可逆矩阵组成的集合，对于矩阵乘法成一个群，称它为域 F 上 n 级**一般线性群**(General Linear Group)，记作 $GL_n(F)$. 名字的由来：给了域 F 上一个 n 级可逆矩阵 A，就决定了 n 维向量空间 F^n 上的一个可逆线性变换 $\mathbf{A}$，它由下式定义：

$$\mathbf{A}(\alpha) = A\alpha, \quad \forall \alpha \in F^n. \tag{25}$$

特别地，域 F 上所有行列式为 1 的 n 级矩阵组成的集合，对于矩阵乘法也成一个群，称它为域 F 上 n 级**特殊线性群**(Special Linear Group)，记作 $SL_n(F)$.

例 10 实数域上所有 n 级正交矩阵组成的集合，对于矩阵的乘

法成一个群,称它为 n 级**正交群**(Orthogonal Group),记作 O_n.

特别地,行列式为 +1 的所有 n 级正交矩阵组成的集合,对于矩阵乘法也成一个群,称它为 n 级**特殊正交群**(Special Orthogonal Group),记作 SO_n.

例 11 复数域上所有 n 级酉矩阵(满足 $A^*A = I$ 的复矩阵 A 称为酉矩阵,其中 $A^* = \bar{A}'$))组成的集合,对于矩阵乘法成一个群,称它为 n 级**酉群**(Unitary Group)记作 U_n. 注意从上下文区分 n 级酉群 U_n 与 n 次单位根群 U_n.

特别地,行列式为 1 的所有 n 级酉矩阵组成的集合,对于矩阵乘法也成一个群,称它为 n 级**特殊酉群**(Special Unitary Group),记作 SU_n.

例 9 至例 11 中的群统称为**矩阵群**(Matrix Groups).

我们常常把 SO_3 看成 3 维**旋转群**(rotation group),这是因为给了一个 3 级矩阵 $A \in SO_3$,由它按照(25)式决定的 $\mathbf{R}^3$ 上的正交变换 $\mathbf{A}$,可以看成是空间中保持原点 O 不动的第一类正交(点)变换,从而它是绕某一条过原点的直线的旋转(参看《解析几何》(第二版),丘维声编,北京大学出版社 1996 年出版,第 235 页的命题 6.1).

例 12 非空集合 Ω 到自身的所有双射组成的集合,对于映射的乘法成一个群,称它为**集合 Ω 的全变换群**(full transformation group),记作 S_Ω.

特别地,当 Ω 为有限集合时,Ω 到自身的一个双射叫做 Ω 的一个**置换**(permutation). 设 Ω 含有 n 个元素,不妨设 $\Omega = \{1,2,\cdots,n\}$,这时 Ω 的一个置换称为 n **元置换**(permutation on n letters),并且称 Ω 的全变换群为 n **元对称群**(symmetric group on n letters),记作 S_n. 名字的由来:以 S_3 为例,下述 3 元多项式

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2, \tag{26}$$

直觉判断它具有对称性. 细致分析:对不定元 x_1, x_2, x_3 作任一置

换，也就是任给集合 $\Omega=\{1,2,3\}$ 上的一个置换 σ，它诱导了 3 元多项式环 $K[x_1,x_2,x_3]$ 到自身的一个映射 $\tilde{\sigma}$：

$$(\tilde{\sigma}f)(x_1,x_2,x_3)\xlongequal{\text{def}}f\left(x_{\sigma^{-1}(1)},x_{\sigma^{-1}(2)},x_{\sigma^{-1}(3)}\right).\tag{27}$$

于是对于(26)式给出的 $f(x_1,x_2,x_3)$，有

$$\begin{aligned}(\tilde{\sigma}f)(x_1,x_2,x_3)&=\!=\!=x_{\sigma^{-1}(1)}^2+x_{\sigma^{-1}(2)}^2+x_{\sigma^{-1}(3)}^2\\&\overset{*}{=\!=}x_1^2+x_2^2+x_3^2\\&=f(x_1,x_2,x_3).\end{aligned}\tag{28}$$

加“*”号这一步相等，是因为 $\sigma^{-1}(1)\sigma^{-1}(2)\sigma^{-1}(3)$ 是 1,2,3 的一个 3 元排列. 从(28)式看出，用 S_3 的所有元素能刻画 3 元多项式 $f(x_1,x_2,x_3)$ 的对称性：不定元 x_1,x_2,x_3 经过任一置换，变成的多项式 $\tilde{\sigma}f$ 与原来的 f 相等. 因此我们把 S_3 叫做 3 元对称群.

注：(27)式右端 x 的下标用 $\sigma^{-1}(i)$，而不用 $\sigma(i)$，这是为了使得

$$\widetilde{\sigma\tau}f=\tilde{\sigma}(\tilde{\tau}f).$$

详述如下：

$$\begin{aligned}&(\widetilde{\sigma\tau}f)(x_1,\cdots,x_n)\\&=f\left(x_{(\sigma\tau)^{-1}(1)},\cdots,x_{(\sigma\tau)^{-1}(1)}\right)\\&=f\left(x_{\tau^{-1}(\sigma^{-1}(1))},\cdots,x_{\tau^{-1}(\sigma^{-1}(n))}\right)\\&=(\tilde{\tau}f)\left(x_{\sigma^{-1}(1)},\cdots,x_{\sigma^{-1}(n)}\right)\\&=[\tilde{\sigma}(\tilde{\tau}f)](x_1,\cdots,x_n).\end{aligned}$$

因此 $\widetilde{\sigma\tau}f=\tilde{\sigma}(\tilde{\tau}f)$.

设 n 元置换 σ 把 i 映成 $a_i(i=1,2,\cdots,n)$，则通常把 σ 写成下述形式：

$$\sigma=\begin{pmatrix}1&2&\cdots&n\\a_1&a_2&\cdots&a_n\end{pmatrix}.\tag{29}$$

由于σ是双射,因此$a_1a_2\cdots a_n$是$1,2,\cdots,n$的一个n元排列.反之,对于任一n元排列$a_1a_2\cdots a_n$,(29)式给出的σ是一个n元置换.因此S_n与所有n元排列组成的集合之间有一个一一对应.由于n元排列的总数为$n!$,因此$|S_n| = n!$.

S_n中任意两个置换相乘是按照映射的乘法进行.以S_4中两个置换σ,τ为例.设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}. \tag{30}$$

则

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}. \tag{31}$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}. \tag{32}$$

我们还可以用一种更节省的方式写出置换.例如,(30)式中的σ,它把$1\mapsto 2,2\mapsto 3,3\mapsto 4,4\mapsto 1$,于是可以把$\sigma$写成下述形式:

$$\sigma = (1\ 2\ 3\ 4). \tag{33}$$

类似地,可以把(30)式中的τ写成

$$\tau = (14)(23). \tag{34}$$

像(1234),(14),(23)这种形式的置换,称为轮换.即:

如果一个n元置换σ把i_1映成i_2,把i_2映成i_3,$\cdots$,把i_{r-1}映成i_r,把i_r映成i_1,并且保持其余的元素不变,则称σ为一个r-**轮换**(r-cycle),简称为**轮换**.记作$(i_1i_2i_3\cdots i_{r-1}i_r)$,也可以写成

$(i_2i_3\cdots i_{r-1}i_ri_1)$，还可以写成$(i_3i_4\cdots i_ri_1i_2)$，等等．特别地，2－轮换也称为**对换**(transposition)．

两个轮换如果它们之间没有公共的元素，则称它们**不相交**(disjoint)．例如，(134)与(25)是不相交的两个轮换．我们来计算它们的乘积．轮换(25)把1，3，4分别保持不变，而轮换(134)分别把2，5保持不变．因此乘积(134)(25)把$1\mapsto 3, 2\mapsto 5, 3\mapsto 4, 4\mapsto 1, 5\mapsto 2$．而乘积(25)(134)也是把$1\mapsto 3, 2\mapsto 5, 3\mapsto 4, 4\mapsto 1, 5\mapsto 2$．因此$(134)(25)=(25)(134)$．这种分析方法对任意两个不相交的轮换都适用，因此我们得到：

不相交的两个轮换对乘法是可交换的．

从把(30)式中的σ,τ写成轮换形式的过程，容易猜想有下述结论：

定理 1 任何一个非单位元的置换都能表示成一些两两不相交的轮换的乘积，并且除了轮换的排列次序外，表示法是唯一的．

证明 设$\sigma\in S_n$，且$\sigma\neq e$．于是在Ω中至少有一个i_1使得$\sigma(i_1)\neq i_1$．设$\sigma(i_1)=i_2, \sigma(i_2)=i_3,\cdots$．由于$|\Omega|=n$，因此在有限步后所得的象必与前面的重复．设$i_r$是第一个与前面出现的象重复的元素，设$i_r=i_j, j<r$．我们断言$j=1$．假如$j>1$，我们有

$$\sigma^{r-1}(i_1)=i_r=i_j=\sigma^{j-1}(i_1). \tag{35}$$

在(35)式两边用σ^{-1}作用，得

$$\sigma^{r-2}(i_1)=\sigma^{j-2}(i_1), \tag{36}$$

即$i_{r-1}=i_{j-1}$．这与i_r的选择矛盾．因此$j=1$．从而$i_r=i_1$．于是得到一个轮换$\sigma_1=(i_1i_2\cdots i_r)$．

在$\Omega\setminus\{i_1,i_2,\cdots,i_r\}$中重复上述步骤，便可得到$\sigma$的轮换分解式：

$$\sigma=\sigma_1\sigma_2\cdots\sigma_t. \tag{37}$$

从上述作法可知，(37)式右边的轮换两两不相交．

唯一性，假设还有

$$\sigma=\tau_1\tau_2\cdots\tau_s, \tag{38}$$

其中 $\tau_1, \tau_2, \cdots, \tau_s$ 是两两不相交的轮换. 任取在 σ 下变动的元素 a，则在 $\sigma_1, \sigma_2, \cdots, \sigma_t$ 中存在唯一的 σ_l，使得 $\sigma_l(a) \neq a$. 同理，在 $\tau_1, \tau_2, \cdots, \tau_s$ 中存在唯一的 τ_k，使得 $\tau_k(a) \neq a$，我们有

$$\sigma_l^m(a) = \sigma^m(a) = \tau_k^m(a), \quad m = 0,1,2,\cdots \tag{39}$$

由于 $\sigma_l = (a\ \ \sigma_l(a)\ \ \sigma_l^2(a)\ \ \cdots)$，$\tau_k = (a\ \ \tau_k(a)\ \ \tau_k^2(a)\ \ \cdots)$，因此 $\sigma_l = \tau_k$. 继续这样的讨论，可得 $t = s$，并且在适当排列 $\tau_1, \tau_2, \cdots, \tau_s$ 的次序后，有 $\sigma_i = \tau_i$，$i = 1,2,\cdots,t$. 从而唯一性成立. □

现在对于(30)式中的 σ、τ，用它们的轮换分解式(33)、(34)来做乘法.

$$\sigma\tau = (1234)(14)(23) = (1)(24)(3) = (24), \tag{40}$$

$$\tau\sigma = (14)(23)(1234) = (13)(2)(4) = (13). \tag{41}$$

像(40)、(41)式那样，在运算的结果中常常把 1 − 轮换省略不写. 单位元素 e 可写成(1)，也可写成(2)，等等.

对于(30)式中的 σ，容易求出它的逆元：

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432). \tag{41}$$

比较 σ 与 σ^{-1} 的轮换表示式，看出

$$(1234)^{-1} = (1432). \tag{42}$$

由此猜想：

$$(i_1, i_2, \cdots, i_{r-1} i_r)^{-1} = (i_1 i_r i_{r-1} \cdots i_2). \tag{43}$$

这可以直接验证如下：

$$\begin{aligned}&(i_1, i_2, \cdots, i_{r-1} i_r)(i_1 i_r i_{r-1} \cdots i_2) \\ &= (i_1)(i_2)(i_3)\cdots(i_{r-1})(i_r);\end{aligned} \tag{44}$$

类似地可以看出它们交换位置后的乘积也等于单位元素. 从而(43)式成立.

通过直接计算可知下式成立：

$$(1234) = (14)(13)(12).$$

一般地,可以直接验证下式成立:

$$(i_1i_2i_3\cdots i_{r-1}i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2). \qquad (45)$$

(45)式表明,每一个轮换可以表示成一些对换的乘积.再结合定理1便得出下述结论:

推论 2 每一个置换都可以表示成一些对换的乘积. □

注意把置换表示成对换的乘积,其表示法不唯一;并且这些对换会相交(即,有公共元素).例如

$$(134)=(14)(13), \qquad (46)$$

$$(134)=(12)(34)(24)(12), \qquad (47)$$

从(46)、(47)式看出,虽然把(134)分解成对换乘积的方式不唯一,但是在这两种分解式里,对换的个数都是偶数,这是不是反映置换的内在性质?我们来探讨这个问题.

设 $\sigma\in S_n$,它分解成对换乘积的一种方式为

$$\sigma=\tau_1\tau_2\cdots\tau_k. \qquad (48)$$

考虑 $x_1,x_2,\cdots,x_n$ 的范德蒙行列式:

$$f(x_1,x_2,\cdots,x_n)=\begin{vmatrix}1 & 1 & \cdots & 1\\ x_1 & x_2 & \cdots & x_n\\ x_1^2 & x_2^2 & \cdots & x_n^2\\ \vdots & & & \vdots\\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1}\end{vmatrix}. \qquad (49)$$

当 $x_1,x_2,\cdots,x_n$ 是 n 个无关不定元时,$f(x_1,x_2,\cdots,x_n)$ 属于 $\mathbf{R}[x_1,x_2,\cdots,x_n]$. S_n 中任一对换 $\tau=(ij)$,它诱导的 $K[x_1,x_2,\cdots,x_n]$ 到自身的映射 $\tilde{\tau}$ 使 $f(x_1,x_2,\cdots,x_n)$ 中的 x_i 与 x_j 互换位置,从而使(49)式右端行列式的第 i 列与第 j 列互换,因此

$$(\tilde{\tau}f)(x_1,x_2,\cdots,x_n)=-f(x_1,x_2,\cdots,x_n). \qquad (50)$$

于是由(48)和(50)式,得

$$(\tilde{\sigma}f)(x_1,x_2,\cdots,x_n)=(-1)^kf(x_1,x_2,\cdots,x_n). \qquad (51)$$

由于(51)式左端只依赖于 σ，因此(51)式右端出现的 $(-1)^k$ 是 $+1$ 还是 -1，完全由 σ 决定，不依赖于 σ 的对换分解式(48)．当 $(-1)^k = +1$ 时，我们称 σ 是**偶置换**(even permutation)；当 $(-1)^k = -1$ 时，称 σ 是**奇置换**(odd permutation)．由此看出，置换 σ 的对换分解式中出现的对换个数 k 的奇偶性是由 σ 本身决定的：当 σ 为偶置换时，对换个数为偶数；当 σ 为奇置换时，对换个数为奇数．于是我们得出下述结论：

命题 3　置换 σ 是偶(奇)置换当且仅当 σ 的对换分解式中对换的个数为偶(奇)数． □

特别地，每一个对换都是奇置换．每一个 3 − 轮换都是偶置换，这是因为 $(ijk) = (ik)(ij)$．

由命题 3 立即得到，两个偶置换的乘积仍是偶置换．从(43)式看到，r − 轮换的逆仍是 r − 轮换．结合定理 1、(45)式以及命题 3 便得出，偶置换的逆还是偶置换．显然单位元素是偶置换．因此 S_n 中所有偶置换组成的集合，对于映射乘法成一个群，称它为 **n 元交错群**(alternating group)，记作 A_n．

由于任一偶置换 σ 与 (12) 的乘积是奇置换，任一奇置换与 (12) 的乘积是偶置换，因此 A_n 与 S_n 中所有奇置换组成的集合之间有一个一一对应．从而 $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$．

习题 1.1

1．写出正十二棱锥(right regular pyramid on a twelve sided base)的旋转对称(性)群的所有元素．这个群是不是循环群？

2．写出正六边形(regular hexagon)的对称(性)群的所有元素．它的生成元是什么？生成元适合的关系有哪些？这个群的阶是多少？

3．正五边形(regular pentagon)的对称(性)群 D_5 为

$$D_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = I,\ \tau\sigma\tau = \sigma^{-1} \rangle,$$

其中 σ 表示绕中心 O 转角为 $\frac{2\pi}{5}$ 的旋转，τ 表示关于某一条对称轴的反射，说出 $\sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau$ 分别表示关于哪一条对称轴的反射；说出 $(\sigma\tau)(\sigma^2\tau)$ 是 D_5 中哪个元素？

4. 写出正四面体(regular tetrahedron)的旋转对称(性)群的所有元素.

*5. 写出正方体(cube)的旋转对称(性)群的所有元素.

6. 写出 $\mathbf{Z}_{15}$ 的单位群 $U(\mathbf{Z}_{15})$ 的全部元素，说出 $U(\mathbf{Z}_{15})$ 的阶是多少？

*7. 设 m 是正整数，在 $0,1,2,\cdots,m-1$ 中，与 m 互素的整数的个数记作 $\varphi(m)$，称它为**欧拉函数**. 证明：$\mathbf{Z}_m$ 的单位群 $U(\mathbf{Z}_m)$ 的阶等于 $\varphi(m)$.

8. 设 3 级实矩阵 A 为

$$A = \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & \frac{2}{3} \\ -\frac{2}{3} & \frac{2}{3} & \frac{1}{3} \\ -\frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \end{pmatrix}.$$

(1) 说明 $A \in SO_3$；

(2) A 可以表示空间中绕哪一条直线的旋转？

9. 在 S_5 中，设

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}.$$

(1) 求 $\sigma_1\sigma_2, \sigma_2\sigma_1$；

(2) 分别写出 σ_1, σ_2 的轮换分解式；

(3) 求 $\sigma_1^{-1}, \sigma_1\sigma_2\sigma_1^{-1}$；

(4) 分别写出 σ_1, σ_2 的一种对换分解式；

(5) 说出 σ_1, σ_2 是偶置换，还是奇置换.

10. r - 轮换是偶置换还是奇置换，与 r 的奇偶性有什么关系?

11. 分别写出 A_3, A_4 的所有元素(用轮换分解式表示)

12. 设 $\sigma = (i_1 i_2 \cdots i_r)$，则对于任意 $\tau \in S_n$，有

$$\tau\sigma\tau^{-1} = (\tau(i_1) \quad \tau(i_2) \quad \cdots \quad \tau(i_r)).$$

§2　子群，陪集，Lagrange 定理，循环群的子群

A_n 是 n 元对称群 S_n 的子集，它对于映射的乘法也成一个群.

$SL_n(F)$ 是一般线性群 $GL_n(F)$ 的子集，它对于矩阵的乘法也成一个群.

SO_n 是正交群 O_n 的子集，它对于矩阵的乘法也成一个群.

像上面这样的许多例子，促使我们抽象出下述概念：

定义 1　群 G 的非空子集 H 如果对于 G 的运算也成一个群，则称 H 为 G 的子群(subgroup).

H 是群 G 的子群可简记为"$H < G$".

实数域上 n 级一般线性群 $GL_n(\mathbf{R})$ 的子群有：$SL_n(\mathbf{R})$，O_n，SO_n. 它们之间的相互关系可以用下图表示：

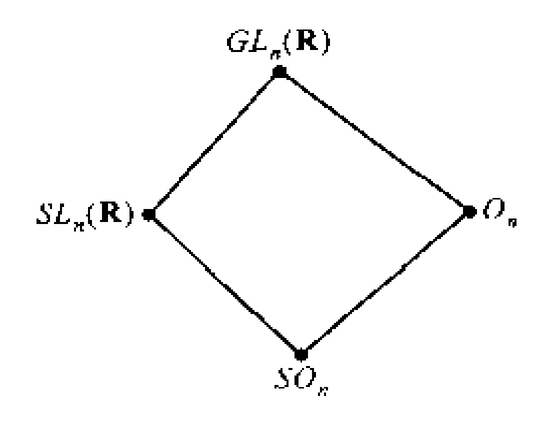


图 1-2

n 元对称群 S_n 的任一子群称为 n 元**置换群**(group of permutations).

非空集合 Ω 的全变换群 S_Ω 的任一子群称为 Ω 的**变换群**(transformation group).

群 G 中,仅由单位元素 e 组成的子集 $\{e\}$ 显然是 G 的一个子群;G 本身也是 G 的子群. $\{e\}$ 和 G 称为 G 的**平凡子群**(trivial subgroups).群 G 的其余子群称为**非平凡的**(non - trivial).

从定义 1 看出,如果 H 是群 G 的子群,则有

(i) $a, b \in H \Longrightarrow ab \in H$;

(ii) G 的单位元素 e 是 H 的单位元;

(iii) $a \in H \Longrightarrow a^{-1} \in H$.

性质(i) 称为 H 对于 G 的运算封闭.性质(ii) 成立的理由如下:设子群 H 的单位元是 e'.则 $e'e' = e'$.两边右乘 e' 在 G 中的逆元 $(e')^{-1}$,得 $e'e'(e')^{-1} = e'(e')^{-1}$.由此得出 $e'e = e$.由于 $e'e = e'$,因此 $e' = e$.关于性质(iii),设 $a \in H$ 在 H 中的逆元为 b,则 $ab = ba = e$.从 G 中看此式得,$b = a^{-1}$.因此 $a^{-1} \in H$.由性质(i) 和(iii) 得,"$a, b \in H \Longrightarrow ab^{-1} \in H$".

反过来,我们有下述子群的判定方法:

命题 1 设 H 是群 G 的非空子集,如果 H 满足:

$$\text{“}a, b \in H \Longrightarrow ab^{-1} \in H\text{”}, \tag{1}$$

则 H 是群 G 的子群.

证明 由于 H 非空,所以 H 中含有一个元素 a.由已知条件得,$aa^{-1} \in H$.即 $e \in H$.

任取 $b \in H$,则 $eb^{-1} \in H$.即 $b^{-1} \in H$.

任取 $c, b \in H$,由于 $b^{-1} \in H$.因此 $c(b^{-1})^{-1} \in H$.即 $cb \in H$.这表明群 G 的运算也是 H 的运算.结合律显然成立.综上述得,H 是 G 的子群. □

由子群的性质以及命题 1,容易得出下述结论:

群 G 的任意子群族 $\{H_i \mid i \in I\}$ 的交 $\bigcap_{i \in I} H_i$ 仍是 G 的子群.

我们可以通过子群来研究群的结构.

从群 G 的一个非空子集 S 出发，我们可以构造出一个包含 S 的最小的子群. 自然的想法是，取 G 的包含 S 的所有子群的交

$$\bigcap_{S \subseteq H < G} H. \tag{2}$$

由上述知，这是 G 的一个子群. 如果 G 的任一子群 K 包含 S，则 K 当然包含上述交集. 因此上述交集的确是 G 的包含 S 的最小的子群. 称它是由 **S 生成的子群**(subgroup generated by S)，记作 $\langle S \rangle$. 此时称 S 是子群 $\langle S \rangle$ 的**生成元集**(set of generators for $\langle S \rangle$).

$\langle S \rangle$ 中的元素是什么样子?

命题 2 设 S 是群 G 的一个非空集合，则

$$\langle S \rangle = \{x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} \mid x_i \in S,\ m_i \in \mathbf{Z},\ 1 \leqslant i \leqslant k,\ k \in \mathbf{Z}^+\}, \tag{3}$$

其中 $x_1, x_2, \cdots, x_k$ 不必是不同的.

证明 把(3)式右端的集合记作 H，显然 $H \supseteq S$. 任取 H 中两个元素：

$$h_1 = x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}, \quad h_2 = y_1^{n_1} y_2^{n_2} \cdots y_l^{n_l},$$

其中 $x_i, y_j \in S, m_i, n_j \in \mathbf{Z}, 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l$. 我们有

$$h_1 h_2^{-1} = x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} y_l^{-n_l} \cdots y_2^{-n_2} y_1^{-n_1} \in H.$$

因此 $H < G$. 由于 $H \supseteq S$，因此 $H \supseteq \langle S \rangle$. 由于 $\langle S \rangle$ 是子群，因此 H 中任一元素属于 $\langle S \rangle$. 从而 $H \subseteq \langle S \rangle$. 因此 $H = \langle S \rangle$. □

特别地，如果 $\langle S \rangle = G$，则称 S 是**群 G 的生成元集**，或者说 **S 的所有元素生成 G**.

如果群 G 有一个生成元集是有限集，则称 G 是**有限生成的群**(finitely generated group). 如果这个生成元集是 $\{a_1, a_2, \cdots, a_t\}$，则记 $G = \langle a_1, a_2, \cdots, a_t \rangle$.

显然,有限群 G 一定是有限生成的(因为 G 本身就是它的一个有限生成元集).反之不对,例如整数加群 $\mathbf{Z}$ 是有限生成的(它由 1 生成),但是 $\mathbf{Z}$ 是无限群.

从 §1 中循环群的定义知道,群 G 是循环群当且仅当 G 由一个元素生成.设 $G=\langle a\rangle$,可分成两种情形:

情形 1 对所有的正整数 m,都有 $a^m\neq e$.此时,如果 $i\neq j$,则 $a^i\neq a^j$.从而 $\langle a\rangle$ 的结构为

$$\langle a\rangle=\{\cdots,a^{-n},\cdots,a^{-2},a^{-1},e,a,a^2,\cdots,a^n,\cdots\}. \tag{4}$$

此时,$\langle a\rangle$ 为无限群.

情形 2 存在正整数 n,使得 $a^n=e$,设 n 是使得 $a^n=e$ 成立的最小正整数,则 $\langle a\rangle$ 的结构为

$$\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}. \tag{5}$$

此时,$\langle a\rangle$ 的阶为 n.

二面体群 D_n 是由两个元素生成的,但要注意:两个元素生成的群不止是二面体群,还有很多群是由两个元素生成的.

n 元对称群 S_n 由几个置换生成?我们作一个初步调查.我们已经知道,S_n 中每个置换可以表示成一些对换的乘积.又任一对换 (ij) 可以表示成

$$(ij)=(1i)(1j)(1i).$$

因此 S_n 可以由 $\{(12),(13),\cdots,(1n)\}$ 生成,即

$$S_n=\langle(12),(13),\cdots,(1n)\rangle. \tag{6}$$

* 思考:S_n 能够由两个元素生成吗?(参看习题 1.2 的第 5 题.)n 元交错群 A_n 可以由哪些置换生成?(参看习题 1.2 的第 6 题.)

群 G 中,由一个元素 a 生成的子群 $\langle a\rangle$ 是循环群.如果 $\langle a\rangle$ 是无限群,则称 a 是**无限阶元素**,记作 $|a|=\infty$.如果 $\langle a\rangle$ 的阶为 n,则称**元素 a 的阶为 n**,记作 $|a|=n$,从上面所讲的循环群的结构立即得出:

群 G 中元素 a 的阶为 ∞ 当且仅当对一切正整数 m,都有 $a^m\neq e$.

群 G 中元素 a 的阶为 n 当且仅当 n 是使 $a^n=e$ 成立的最小正整数.

S_n 中，设 $\sigma=(a_1a_2\cdots a_r)$，则 $\sigma^r=(1)$；而当 $1\leqslant l<r$ 时，$\sigma^l\neq(1)$. 因此 σ 的阶为 r，即 r-轮换的阶为 r.

域 F 的单位元用 e 表示. 如果 e 在 F 的加法群中的阶为 ∞，则称域 F 的**特征为** 0(characteristic 0)；如果 e 在 F 的加法群中的阶为正整数 p，则称域 F 的**特征为** p(characteristic p). 域 F 的特征记作 char F. 可以证明：域 F 的特征或者为 0，或者为一个素数. 还可以证明：域 F 的任一非零元 a 与 e 在加法群中的阶相同.（这些证明可参看《高等代数(下册)》，丘维声编著，高等教育出版社 1996 年出版，第 151 页.）

元素的阶这个概念对于研究群的结构会有帮助. 这里我们给出有关元素的阶的几个常用结论.

命题 3 群 G 中，设元素 a 的阶为 n. 则

(1) $a^m=e$ 当且仅当 $n\mid m$；

(2) 对于任意正整数 k，有 $|a^k|=\dfrac{n}{(n,k)}$.

证明 (1) 必要性. 设 $a^m=e$. 作带余除法：

$$m=ln+r,\quad 0\leqslant r<n.$$

则 $e=a^m=a^{ln+r}=a^{ln}a^r=ea^r=a^r$.

由于 $|a|=n$，从上式得出 $r=0$. 因此 $n\mid m$.

充分性. 设 $m=ln$，则 $a^m=a^{ln}=e$.

(2) 设 $|a^k|=s$. 设 $n=n_1(n,k)$，$k=k_1(n,k)$. 则 $(n_1,k_1)=1$，由于

$$(a^k)^{n_1}=a^{k_1(n,k)n_1}=a^{k_1n}=e,$$

因此 $s\mid n_1$. 由于 $e=(a^k)^s=a^{ks}$，因此 $n\mid ks$. 即 $n_1(n,k)\mid k_1(n,k)s$. 从而 $n_1\mid k_1s$. 由于 $(n_1,k_1)=1$，因此 $n_1\mid s$，综上述得，$s=n_1=\dfrac{n}{(n,k)}$. □

命题 4　设群 G 中元素 a,b 的阶分别为 n,m，如果 $ab=ba$，且 $(n,m)=1$，则 ab 的阶等于 nm.

证明　由于 $ab=ba$，因此

$$(ab)^{nm}=a^{nm}b^{nm}=(a^n)^m(b^m)^n=e.$$

由此得出，ab 是有限阶元素，并且 ab 的阶 $s\mid nm$.

由于 $(ab)^s=e$，因此

$$e=(ab)^{sn}=a^{sn}b^{sn}=b^{sn}.$$

由此得出，$m\mid sn$. 由于 $(m,n)=1$，因此 $m\mid s$. 同理可证 $n\mid s$. 仍然由于 $(m,n)=1$，因此 $mn\mid s$.

综上述得，$s=nm$. □

例如，在 6 阶循环群 $G=\langle a\rangle$ 中，

$$|a^2|=\frac{6}{(6,2)}=3,\quad |a^3|=\frac{6}{(6,3)}=2,\quad |a^4|=\frac{6}{(6,4)}=3,$$

$$|a^5|=|a^2a^3|=3\times 2=6.$$

从上述 6 阶循环群 $\langle a\rangle$ 的例子看到，$|a|=|a^5|=6$，$|a^2|=|a^4|=3$，$|a^3|=2$，$|e|=1$. 这表明 $\langle a\rangle$ 的每个元素的阶都是群 $\langle a\rangle$ 的阶的因子.

任意一个有限群，它的元素的阶是否都是群的阶的因子？为了回答这一问题，以及为了研究群（不论是有限群还是无限群）的结构，我们将利用子群给出群的一个划分，然后通过这个划分来研究群的结构.

把一个集合划分，这是日常生活中常见的现象. 例如，庆贺某一位同学过生日时，把生日蛋糕切成许多小块；人们为了劳逸结合，把整数集划分成“星期一”，“星期二”，…，“星期六”，“星期日”等 7 个子集.

如何给出集合的一个划分？一个非常有效的方法是，在集合 S 上建立一个等价关系，那么所有等价类组成的集合就是 S 的一个划分（参看《高等代数（第二版）上册》，丘维声，高等教育出版社 2002 年

7月出版，第159页的定理2）.

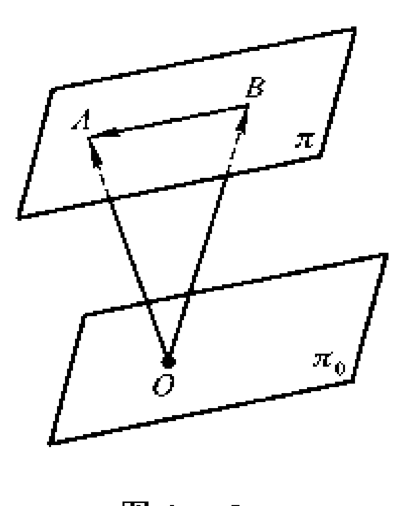


图1-3

例如在几何空间中，如果给了一个过原点 O 的平面 π_0，那么 π_0 以及与 π_0 平行的所有平面组成的集合就是几何空间的一个划分，其中每一个平面是下述等价关系的一个等价类：

$$\overrightarrow{OA} \sim \overrightarrow{OB} \overset{\text{def}}{\iff} \overrightarrow{OA} - \overrightarrow{OB} \in \pi_0.$$

从这个例子受到启发，对于群 G，利用它的一个子群 H，定义一个二元关系如下：对于 $a,b \in G$，规定

$$a \sim b \overset{\text{def}}{\iff} b^{-1}a \in H. \tag{7}$$

由(7)式定义的关系～是一个等价关系，证明如下：

(i) 反身性. 任取 $a \in G$，有 $a^{-1}a = e \in H$，因此 $a \sim a$.

(ii) 对称性. 设 $a \sim b$，则 $b^{-1}a \in H$，从而 $(b^{-1}a)^{-1} \in H$，即 $a^{-1}b \in H$. 因此 $b \sim a$.

(iii) 传递性. 设 $a \sim b, b \sim c$，则 $b^{-1}a, c^{-1}b \in H$，从而 $(c^{-1}b)(b^{-1}a) \in H$，即 $c^{-1}a \in H$. 因此 $a \sim c$. □

上述等价关系～就可以给出群 G 的一个划分. 为此我们来求等价类. a 确定的等价类 $\bar{a}$ 为

$$\bar{a} = \{x \in G \mid x \sim a\} = \{x \in G \mid a^{-1}x \in H\}$$

$$= \{x \in G \mid a^{-1}x = h, h \in H\}$$
$$= \{x \in G \mid x = ah, h \in H\}$$
$$= \{ah \mid h \in H\}.$$

令

$$aH \xlongequal{\text{def}} \{ah \mid h \in H\}. \tag{8}$$

称 aH 是子群 H 的一个**左陪集**(left coset)，a 称为左陪集 aH 的一个代表. 子群 H 本身是一个左陪集(因为 $H = eH$)，e 是左陪集 H 的一个代表.

上述推导过程表明，a 确定的等价类 $\bar{a}$ 就是左陪集 aH. 于是从等价类的有关性质立即得出左陪集的性质：

性质 1 $aH = bH \Longleftrightarrow b^{-1}a \in H$；

性质 2 子群 H 的任意两个左陪集或者相等，或者不相交(即它们的交集为空集).

上述两条性质可参看《高等代数(第二版) 上册》(丘维声编著，高教社 2002 年 7 月出版)第 159 页的事实 4 和定理 1. 从性质 1 看出，同一个左陪集里的任何一个元素都可作为这个左陪集的一个代表.

群 G 中，子群 H 的所有左陪集组成的集合就是 G 的一个划分.

群 G 中，子群 H 的所有左陪集组成的集合称为 G 关于 H 的**左商集**(left quotient set)，记作 $(G/H)_l$.

类似地，对于 $a, b \in G$，规定

$$a \sim b \overset{\text{def}}{\Longleftrightarrow} ab^{-1} \in H, \tag{9}$$

则这个二元关系 ~ 也是一个等价关系. 此时容易推导出

$$\bar{a} = \{ha \mid h \in H\}.$$

令

$$Ha \xlongequal{\text{def}} \{ha \mid h \in H\}. \tag{10}$$

称 Ha 是子群 H 的一个**右陪集**(right coset).

从等价类的有关性质可得出右陪集的性质. 例如，

$$Ha = Hb \Longleftrightarrow ab^{-1} \in H. \tag{11}$$

群 G 中，子群 H 的所有右陪集组成的集合也是 G 的一个划分．这个集合称为 G 关于 H 的**右商集**(right quotient set)，记作 $(G/H)_r$．

群 G 关于子群 H 的左商集与右商集之间有什么关系？令

$$f:(G/H)_l \longrightarrow (G/H)_r,$$
$$aH \longmapsto Ha^{-1}.$$

由于

$$aH = bH \Longleftrightarrow b^{-1}a \in H \Longleftrightarrow (b^{-1})(a^{-1})^{-1} \in H$$
$$\Longleftrightarrow Hb^{-1} = Ha^{-1},$$

因此 f 是映射，并且是单射．显然 f 是满射，从而 f 是双射．即左商集 $(G/H)_l$ 与右商集 $(G/H)_r$ 之间有一个一一对应．

集合有**基数**(cardinal number)的概念．如果两个集合之间有一个一一对应，则称这两个集合有相同的基数．例如，**N**，**Z**，**Q** 有相同的基数，而 **Q** 与 **R** 的基数不同，我们用 $|\Omega|$ 表示集合 Ω 的基数．当 Ω 为无限集时，记 $|\Omega| = \infty$．注意两个无限集的基数虽然都记成 ∞，但是它们有可能不相同．当 Ω 为有限集时，Ω 的基数 $|\Omega|$ 等于 Ω 所含元素的个数．

上述表明，群 G 关于子群 H 的左商集与右商集有相同的基数．

群 G 关于子群 H 的左商集（或右商集）的基数称为 H 在 G 中的**指数**(index)，记作 $[G:H]$．

如果群 G 的子群 H 在 G 中的指数 $[G:H]=r$，则由于 H 的所有左陪集组成的集合是 G 的一个划分，因此有

$$G = H \cup a_1H \cup a_2H \cup \cdots \cup a_{r-1}H, \tag{12}$$

其中 $H, a_1H, a_2H, \cdots, a_{r-1}H$ 两两不相交，我们称(12)式是群 G 关于子群 H 的**左陪集分解式**．$\{e, a_1, a_2, \cdots, a_{r-1}\}$ 称为 H 在 G 中的**左陪集代表系**，我们常常把 e 写成 a_0．

显然，在子群 H 与它的任意一个左陪集 aH 之间有一个双射：

$h \mapsto ah$. 因此 $|H| = |aH|$, $\forall a \in G$. 利用这个结论和(12)式,我们可以得出下述重要结论:

定理 5(Lagrange 定理) 有限群 G 的任一子群 H 的阶必为群 G 的阶的因子. 更精确地,我们有

$$|G| = |H|[G:H]. \tag{13}$$

证明 从群 G 关于子群 H 的左陪集分解式(12)得,

$$|G| = \sum_{i=0}^{r-1} |a_i H| = \sum_{i=0}^{r-1} |H| = |H| r = |H| [G:H]. \quad \square$$

推论 6 有限群 G 的每一个元素的阶是 G 的阶的因子. 设 $|G| = m$, 则 $a^m = e$, $\forall a \in G$.

证明 任取 $a \in G$, 我们有 $|a| = |\langle a \rangle|$, 从而 $|a|$ 是 $|G|$ 的因子.

设 $|G| = m$, 由于 $|a| \mid m$, 因此 $a^m = e$. $\square$

推论 7 素数阶群一定是循环群.

证明 设群 G 的阶是素数 p. 于是 G 中有非单位元 a. 由于 $|a| \mid p$, 因此 $|a| = p$. 于是 $G = \langle a \rangle$. $\square$

利用推论 6, 我们可以给出数论中费马小定理(Fermat's Little Theorem)一个简短的证明.

定理 8(费马小定理) 如果 p 是素数,并且 a 不是 p 的倍数,则

$$a^{p-1} \equiv 1 \pmod{p}. \tag{14}$$

证明 由于 a 不是 p 的倍数,因此 $\bar{a} \in \mathbf{Z}_p^*$, 由于 $|\mathbf{Z}_p^*| = p - 1$, 据推论 6 得 $\bar{a}^{p-1} = \bar{1}$, 即 $\overline{a^{p-1}} = \bar{1}$. 从而 $a^{p-1} \equiv 1 \pmod{p}$. $\square$

现在我们能够决定有限循环群的所有子群.

定理 9 设 $G = \langle a \rangle$ 是 n 阶循环群,则

(1) G 的每一个子群都是循环群;

(2) 对于 G 的阶 n 的每一个正因子 s, 都存在唯一的一个 s 阶子群,它们就是 G 的全部子群.

证明 (1) 设 H 是 G 的非平凡子群,则 H 中有 G 的非单位元.

于是在 H 中存在幂指数最小的 a 的方幂，设为 a^k，$k \neq 0$. 任取 $a^q \in H$. 设

$$q = lk + r, \quad 0 \leqslant r < k,$$

则

$$a^r = a^{q-lk} = a^q(a^k)^{-l} \in H.$$

假如 $r \neq 0$，则上式与 a^k 的取法矛盾，因此 $r = 0$，从而 $a^q = (a^k)^l \in \langle a^k \rangle$. 于是 $H \subseteq \langle a^k \rangle$. 从而 $H = \langle a^k \rangle$.

G 的平凡子群 $\{e\}$，G 显然是循环群.

（2）设 s 是 G 的阶 n 的任一正因子，则存在正整数 d，使得 $n = ds$. 由于 $|a| = n$，据命题 3 得

$$|a^d| = \frac{n}{(n,d)} = \frac{n}{d} = s.$$

因此 $\langle a^d \rangle$ 是 G 的一个 s 阶子群.

设 H 是 G 的任意一个 s 阶子群，据(1)的结论知，H 是循环群. 设 $H = \langle a^k \rangle$，于是 $|a^k| = s = \frac{n}{d}$. 又有 $|a^k| = \frac{n}{(n,k)}$，因此 $(n,k) = d$. 从而存在 $u, v \in \mathbf{Z}$，使得

$$un + vk = d. \tag{15}$$

于是

$$a^d = a^{un+vk} = a^{un}a^{vk} = (a^k)^v \in \langle a^k \rangle,$$

从而 $\langle a^d \rangle \subseteq \langle a^k \rangle$. 又由于它们的阶都等于 s，因此 $\langle a^d \rangle = \langle a^k \rangle = H$. 这证明了 G 的 s 阶子群唯一.

据 Lagrange 定理，n 阶群 G 的每一个子群的阶都是 n 的因子，因此上述得到的子群就是循环群 G 的全部子群. □

从上述证明过程中看出，设 $d \mid n$，如果 $(n,k) = d$，则 $\langle a^k \rangle = \langle a^d \rangle$. 特别地，当 $d = 1$ 时，我们可以得出：

$$\langle a^k \rangle = \langle a \rangle \Longleftrightarrow (n,k) = 1.$$

从而 n 阶循环群 $\langle a \rangle$ 的生成元恰好有 $\varphi(n)$ 个，其中 $\varphi(n)$ 是欧拉函数，它是 $0, 1, 2, \cdots, n-1$ 中与 n 互素的整数的个数.

循环群一定是 abel 群，反之不对．现在我们利用定理 9 以及有关元素的阶的结论，探索有限 abel 群为循环群的条件，首先我们给出有限 abel 群中元素的阶的性质．

命题 10　设 G 为有限 abel 群，则 G 中存在一个元素，它的阶是 G 中所有元素的阶的倍数．

证明　设 a 是有限 abel 群 G 中阶最大的一个元素，a 的阶为 n．假如 G 中有一个元素 b，使得 b 的阶 m 不能整除 n，则存在一个素数 p 满足

$$p^r \mid m, \quad 但\ p^r \nmid n.$$

设 $m = lp^r, n = kp^s$，其中 $0 \leqslant s < r$，$(k,p) = 1$．由于 $|b^l| = \dfrac{m}{(m,l)} = p^r$，$|a^{p^s}| = \dfrac{n}{(n,p^s)} = k$，且 $(p^r,k) = 1$，$ab = ba$，因此据命题 4 得

$$|b^l a^{p^s}| = p^r k > p^s k = n.$$

这与 a 是最大阶元素矛盾．因此 G 中所有元素的阶都能整除 n．□

现在我们可以给出有限 abel 群为循环群的条件．

定理 11　设 G 为有限 abel 群，则 G 为循环群当且仅当对于任一正整数 m，方程 $x^m = e$ 在 G 中的解的个数不超过 m．

证明　充分性．据命题 10，G 中有一个元素 a，它的阶 n 是 G 中所有元素的阶的倍数，从而 G 中每一个元素都是方程 $x^n = e$ 的解．由已知条件得 $|G| \leqslant n$．又由于 $\langle a \rangle \subseteq G$，因此 $n \leqslant |G|$．从而 $|G| = n$．于是 $G = \langle a \rangle$．

必要性．设 $G = \langle a \rangle$ 的阶为 n．对于任一正整数 m，令

$$H = \{x \in G \mid x^m = e\}.$$

显然 $e \in H$．对于任意 $b, c \in H$，有 $(bc^{-1})^m = b^m c^{-m} = e$，因此 $bc^{-1} \in H$，从而 $H < G$．据定理 9 得，$H = \langle a^d \rangle$，其中 d 是 n 的一个正因子，且 H 的阶 $s = \dfrac{n}{d}$．据 H 的定义得，$(a^d)^m = e$．由于 a^d 的阶为 s，

因此 $s \leq m$. 从而 $s \leq m$，即 $|H| \leq m$. 这就证明了方程 $x^m = e$ 在 G 中的解的个数不超过 m. □

定理 11 有重要应用.

定理 12 有限域 F 的乘法群 F^* 必为循环群.

证明 由于域 F 上 m 次多项式 $f(x)$ 在 F 中至多有 m 个根(重根按重数计算)，因此对于任一正整数 m，方程 $x^m = e$ 在 F^* 中的解的个数不超过 m(显然 0 不是 $x^m = e$ 的解). 由于 F^* 是有限 abel 群，因此据定理 11 得，F^* 必为循环群. □

利用定理 12 和定理 9，我们可以给出数论中 Wilson 定理一个群论的证明(在习题 1.6 的第 13 题还将给出 Wilson 定理的另一个群论的证明).

定理 13(Wilson 定理) 设 p 是素数，则

$$(p-1)! \equiv -1 \pmod{p}. \tag{16}$$

证明 如果 $p = 2$，则(16)式显然成立. 下面设 p 是奇素数. 据定理 12 得，$\mathbf{Z}_p^*$ 为循环群. $\mathbf{Z}_p^*$ 的阶 $p-1$ 为偶数，因此 $\mathbf{Z}_p^*$ 有**唯一**的 2 阶子群，从而有唯一的 2 阶元. 由于 $\overline{-1}^2 = \overline{1}$，且 $\overline{-1} \neq \overline{1}$，因此 $\overline{-1}$ 是 2 阶元.

在群 $\mathbf{Z}_p^*$ 中，设 $a_1, a_2, \cdots, a_{p-1}$ 分别是 $\overline{1}, \overline{2}, \cdots, \overline{p-1}$ 的逆元，则

$$(\overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1})(a_1 a_2 \cdots a_{p-1}) = \overline{1}. \tag{17}$$

由于群中不同元素的逆元不相等，因此

$$\{a_1, a_2, \cdots, a_{p-1}\} = \{\overline{1}, \overline{2}, \cdots, \overline{p-1}\}. \tag{18}$$

从(17)、(18)式得，

$$(\overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1})^2 = \overline{1}. \tag{19}$$

如果能证明 $\overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1} \neq \overline{1}$，则 $\overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1}$ 是 2 阶元. 因此

$$\overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1} = \overline{-1}. \tag{20}$$

即
$$\overline{1 \cdot 2 \cdot \cdots \cdot (p-1)} = \overline{-1}.$$

从而 $$(p-1)! \equiv -1 \pmod{p}.$$

现在来证 $\bar{1}\cdot\bar{2}\cdot\cdots\cdot\overline{p-1}\neq\bar{1}$. 由于 $\mathbf{Z}_p^*$ 是 $p-1$ 阶循环群，因此它可以写成

$$\mathbf{Z}_p^* = \{e, a, a^2, \cdots, a^{p-2}\}. \tag{21}$$

假如 $\bar{1}\cdot\bar{2}\cdot\cdots\cdot\overline{p-1}=\bar{1}$，则

$$e = e\cdot a\cdot a^2\cdot\cdots\cdot a^{p-2} = a^{\frac{(p-1)(p-2)}{2}}. \tag{22}$$

由于 a 的阶为 $p-1$，因此从(22)式得

$$(p-1) \mid \frac{1}{2}(p-1)(p-2). \tag{23}$$

从(23)式得出，$p-2=2l$，对于某个整数 l. 这与 p 是奇数矛盾.

□

习题 1.2

1. 设 k 是一个非负整数，令

$$k\mathbf{Z} \xlongequal{\text{def}} \{km \mid m \in \mathbf{Z}\}.$$

(1) 说明 $k\mathbf{Z}$ 是整数加群 $\mathbf{Z}$ 的子群；

(2) 说明 $k\mathbf{Z}$ 是循环群.

2. 设 H, K 都是群 G 的子群，令

$$HK \xlongequal{\text{def}} \{hk \mid h \in h, k \in K\}.$$

证明：HK 为子群当且仅当 $HK = KH$.

3. 在复数加群 $\mathbf{C}$ 中，由 $1, i$ 生成的子群 $\langle 1, i\rangle$ 称为**高斯整数群**(group of Gaussian integers)，它的元素是什么样子？

4. 如图 1－4 是一个正方形的棋盘，求它的对称(性)群.

*5. 证明：

(1) $S_n = \langle (12), (23), \cdots, (n-1\ n)\rangle$；

(2) $S_n = \langle (12), (12\cdots n)\rangle$.

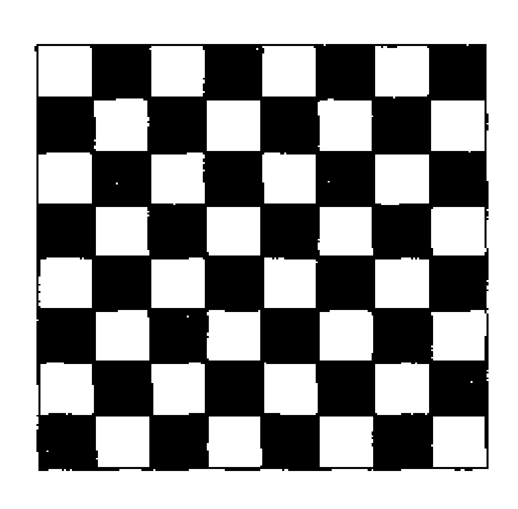


图 1－4

6. 证明：当 $n \geq 3$ 时，

(1) A_n 由 3－轮换生成；

*(2) $A_n = \langle (123),(124),\cdots,(12n) \rangle$.

7. 在 $SL_2(\mathbf{Q})$ 中，设

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

证明：A 的阶为 4，B 的阶为 3，AB 为无限阶元素.

8. 证明：如果群 G 的每一个非单位元的阶都为 2，则 G 必为 abel 群.

*9. 证明：如果群 G 的阶为偶数，则 G 必有 2 阶元.

*10. 证明欧拉(Euler)定理：设 n 是正整数，如果整数 a 与 n 互素，则

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

其中 $\varphi(n)$ 是欧拉函数.

11. 求 6 阶循环群 $G = \langle a \rangle$ 的所有子群.

12. 求 S_3 的所有子群.

13. (1) 写出 A_4 的所有子群；

*(2) 证明 A_4 没有 6 阶子群.

*14. 设 H, K 是群 G 的有限子群,证明:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

§3 群的同构,群的直积

我们已经认识了一些群.世界上的群多种多样,使人眼花瞭乱,如何辨认哪些群在本质上是一样的,哪些群在本质上是不同的?对于本质上一样的群,只要拿一个比较熟悉的群来研究就可以了,起到事半功倍的效果.进一步,数学家们的宏伟目标是想了解世界上有多少本质上不同的群.

什么样的两个群在本质上是一样的?让我们来看一个例子.二次单位根群 $U_2 = \{1, -1\}$ 的乘法表,与 $\mathbf{Z}_2$ 的加法表分别如下:

	1	−1
1	1	−1
−1	−1	1

	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

把 U_2 的乘法表中的 1, −1 分别换成 $\bar{0}, \bar{1}$,便得到 $\mathbf{Z}_2$ 的加法表,这表明 U_2 与 $\mathbf{Z}_2$ 除了元素的名称不同,运算的名称和定义不同外,其它都是一样的.也就是说,群 U_2 与 $\mathbf{Z}_2$ 在本质上是一样的.说得具体一点就是,U_2 与 $\mathbf{Z}_2$ 的元素之间有一个一一对应:$1 \mapsto \bar{0}$, $-1 \mapsto \bar{1}$,并且 U_2 的任意两个元素的乘积对应于它们在 $\mathbf{Z}_2$ 中对应的元素的和.由此受到启发,抽象出下述概念:

定义 1 设 G 和 G' 是两个群.如果 G 到 G' 有一个双射 σ,使得对于 G 中任意两个元素 a, b,都有

$$\sigma(ab) = \sigma(a)\sigma(b), \tag{1}$$

那么称群 G 与 G' 是**同构的**(isomorphic),记作 $G \cong G'$;称 σ 是 G 到

G' 的一个**同构映射**,简称为**同构**(isomorphism).

由上面的议论知道,$U_2 \cong \mathbf{Z}_2$. U_2 是 2 阶循环群,$\mathbf{Z}_2$ 也是 2 阶循环群,是不是任何一个 2 阶循环群都和 $\mathbf{Z}_2$ 同构?更一般地,是不是任意一个 m 阶循环群都与 $\mathbf{Z}_m$ 同构?无限循环群与哪个(些)群同构?下面的定理 1 回答了这些问题.

定理 1 任意一个无限循环群都与 $\mathbf{Z}$ 同构;任意一个 m 阶循环群都与 $\mathbf{Z}_m$ 同构.

证明 设 $G = \langle a \rangle$ 是无限循环群,则

$$G = \{a^k \mid k \in \mathbf{Z}\}$$

建立 G 到 $\mathbf{Z}$ 的一个映射 $\sigma: a^k \mapsto k$,显然 σ 是双射,并且有

$$\sigma(a^k \cdot a^l) = \sigma(a^{k+l}) = k + l = \sigma(a^k) + \sigma(a^l).$$

因此 $G \cong \mathbf{Z}$.

现在设 $G = \langle a \rangle$ 是 m 阶循环群,则

$$G = \{e, a, a^2, \cdots, a^{m-1}\}.$$

建立 G 到 $\mathbf{Z}_m$ 的一个映射 $\sigma: a^k \mapsto \bar{k}$, $0 \leqslant k \leqslant m-1$. 显然 σ 是满射. 我们来证 σ 是单射:设 $\bar{k} = \bar{l}$,则 $\overline{k-l} = \bar{0}$. 从而 $k - l = qm$. 于是

$$a^{k-l} = a^{qm} = e.$$

由此得出,$a^k = a^l$. 因此 σ 是单射. 我们有

$$\sigma(a^k a^l) = \sigma(a^{k+l}) = \overline{k+l} = \bar{k} + \bar{l} = \sigma(a^k) + \sigma(a^l).$$

因此,G 与 $\mathbf{Z}_m$ 同构. □

从定理 1,我们对所有的循环群就了如指掌了. 对于无限循环群,就拿 $\mathbf{Z}$ 作为代表;对于 m 阶循环群,就拿 $\mathbf{Z}_m$ 作为代表. 今后当我们说 $\mathbf{Z}_m$ 是群时,指的就是 $\mathbf{Z}_m$ 的加法群,不再每一次声明.

显然,群的同构作为群之间的一种关系具有反身性、对称性和传递性,即它是一个等价关系. 此时,等价类称为同构类. 这个等价关系给出了所有群组成的集合的一个划分.

从定理 1 以及同构关系的对称性和传递性得出,任意两个无限循环群都同构;任意两个 m 阶循环群都同构,其中 m 是正整数.

由于群 G 与群 G' 同构的一个必要条件是，G 到 G' 有一个双射，从而它们的基数相同．因此基数不同的两个群一定不同构．由此知道，无限群与有限群不同构；阶不同的两个有限群不同构．

由于群 G 与群 G' 同构的另一个必要条件是，G 到 G' 有一个映射 σ 保持运算，因此 G 与 G' 中由运算决定的性质是一样的．例如，G 与 G' 同为交换群，或者同为非交换群．由此知道，非交换群与交换群一定不同构．

命题 2 设 σ 是群 G 到群 G' 的一个同构映射，则

(1) σ 把 G 的单位元 e 映成 G' 的单位元 e'；

(2) 对于任意 $a \in G$，有 $\sigma(a^{-1}) = \sigma(a)^{-1}$；

(3) 对于任意 $a \in G$，a 与 $\sigma(a)$ 的阶相同（即，或者同为无限阶元素，或者它们的阶是同一个正整数）；

(4) G 的子群 H 在 σ 下的象 $\sigma(H)$ 是 G' 的子群．

证明 (1) 我们有

$$\sigma(e)\sigma(e) = \sigma(ee) = \sigma(e),$$

上式两边同时左乘 $\sigma(e)$ 在 G' 中的逆，得

$$e'\sigma(e) = e'. \tag{2}$$

由于 $e'\sigma(e) = \sigma(e)$，因此从(2)式得，$\sigma(e) = e'$．

(2) 由于 $\sigma(a)\sigma(a^{-1}) = \sigma(aa^{-1}) = \sigma(e) = e'$，在此式两边左乘 $\sigma(a)^{-1}$，得 $\sigma(a^{-1}) = \sigma(a)^{-1}$．

(3) 由于 σ 是单射且保持运算，因此对于任意正整数 n，有

$$\begin{aligned} a^n = e &\Longleftrightarrow \sigma(a^n) = \sigma(e) \\ &\Longleftrightarrow [\sigma(a)]^n = e'. \end{aligned} \tag{3}$$

由此推出，a 与 $\sigma(a)$ 或者都为无限阶元素，或者它们的阶是同一个正整数．

(4) 由于 $e' = \sigma(e) \in \sigma(H)$，因此 $\sigma(H)$ 非空．对于 $\sigma(H)$ 中任意两个元素 a', b'，存在 $a, b \in H$，使得 $\sigma(a) = a'$，$\sigma(b) = b'$．由于 $ab^{-1} \in H$，因此有

$$a'b'^{-1} = \sigma(a)\sigma(b)^{-1} = \sigma(a)\sigma(b^{-1}) = \sigma(ab^{-1}) \in \sigma(H).$$

从而 $\sigma(H)$ 是 G' 的子群. □

我们已经知道,素数阶群一定是循环群,因此 2 阶群,3 阶群,5 阶群,7 阶群等都是循环群,从而 2 阶群恰有一个同构类,3 阶群恰有一个同构类,5 阶群,7 阶群也类似. 自然会问:4 阶群有多少个同构类?

$\mathbf{Z}_4$ 是 4 阶循环群.

A_4 有一个 4 阶子群 K:

$$K = \{(1),(12)(34),(13)(24),(14)(23)\}.$$

K 中非单位元都是 2 阶元,K 没有 4 阶元. 而 $\mathbf{Z}_4$ 有 4 阶元 $\bar{1}$. 因此 K 与 $\mathbf{Z}_4$ 不同构,从而 4 阶群至少有两个同构类. 还有其他的同构类吗?

设 G 是任意一个 4 阶群,则 G 中非单位元的阶只可能是 4 或 2.

情形 1 G 有 4 阶元 a,则 $G = \langle a\rangle$. 从而

$$G \cong \mathbf{Z}_4.$$

情形 2 G 没有 4 阶元. 则 G 的 3 个非单位元 a,b,c 都是 2 阶元. 容易看出,$ab \neq e$(否则 $a = b^{-1}$,又 $b^{-1} = b$,于是 $a = b$,矛盾);$ab \neq a$;$ab \neq b$. 因此 $ab = c$. 同理 $ba = c$. 于是 $ab = ba$. 由于 a,b,c 的地位是一样的,因此同理可证

$$ac = b = ca, \quad bc = a = cb.$$

从而 G 是 abel 群. 令

$$\begin{aligned} \sigma: G &\longrightarrow K \\ e &\longmapsto (1) \\ a &\longmapsto (12)(34) \\ b &\longmapsto (13)(24) \\ c &\longmapsto (14)(23) \end{aligned}$$

由于

$$[(12)(34)][(13)(24)] = (14)(23),$$

$$[(12)(34)][(14)(23)] = (13)(24),$$
$$[(13)(24)][(14)(23)] = (12)(34),$$

等. 因此 σ 是 G 到 K 的一个同构映射. 从而 $G \cong K$.

综上所述, 4 阶群恰有两个同构类: 一类是 4 阶循环群, 它的代表是 $\mathbf{Z}_4$; 另一类是 4 阶非循环的 abel 群, 它的代表可以取 A_4 的 4 阶子群 K. 有没有更简单的 4 阶非循环的 abel 群作为代表?

我们来考虑 $\mathbf{Z}_2$ 与自身的笛卡儿积:

$$\mathbf{Z}_2 \times \mathbf{Z}_2 = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}. \tag{4}$$

规定

$$(a_1,a_2)+(b_1,b_2) \xlongequal{\text{def}} (a_1+b_1,a_2+b_2), \tag{5}$$

其中 $a_i,b_i \in \mathbf{Z}_2, i=1,2$.

显然, $\mathbf{Z}_2 \times \mathbf{Z}_2$ 对于上述运算成为一个 abel 群, 它的单位元是 $(\bar{0},\bar{0})$. 由于

$$2(\bar{0},\bar{1}) = (\bar{0},\bar{1})+(\bar{0},\bar{1}) = (\bar{0},\bar{0}),$$

因此 $(\bar{0},\bar{1})$ 是 2 阶元. 类似地, $(\bar{1},\bar{0})$, $(\bar{1},\bar{1})$ 也是 2 阶元. 从而 $\mathbf{Z}_2 \times \mathbf{Z}_2$ 是一个 4 阶非循环的 abel 群, 称它为 **Klein 群**, 也称为**四群**(德文是 Vierergruppe), 记作 V. 它可以作为 4 阶非循环的 abel 群的代表.

从 $\mathbf{Z}_2 \times \mathbf{Z}_2$ 的构造受到启发, 我们来考虑一般情形.

设 G 和 G' 是两个群, 在它们的笛卡儿积 $G \times G'$ 上定义一个二元运算如下:

$$(g_1,g_1')(g_2,g_2') \xlongequal{\text{def}} (g_1g_2,g_1'g_2'). \tag{6}$$

显然, 这个运算满足结合律, 有单位元 (e,e'), 每个元素 (g,g') 有逆元 (g^{-1},g'^{-1}). 因此 $G \times G'$ 成为一个群, 称它为群 G 与 G' 的**直积**(direct product), 记作 $G \times G'$.

如果群 G 与 G' 的运算都记成加法, 则直积 $G \times G'$ 的运算也记成加法. 此时也称直积 $G \times G'$ 是群 G 与 G' 的**直和**(direct sum), 记成 $G \oplus G'$.

显然，如果 G(或 G')是无限群，则直积 $G\times G'$ 也是无限群．如果 G 和 G' 都是有限群，则直积 $G\times G'$ 也是有限群，并且 $|G\times G'|=|G||G'|$．

显然，如果 G 和 G' 都是 abel 群，则直积 $G\times G'$ 也是 abel 群．

显然，直积 $G\times G'$ 与 $G'\times G$ 同构，因为 $(g,g')\mapsto(g',g)$ 是 $G\times G'$ 到 $G'\times G$ 的一个同构映射．

容易验证，$G\times G'$ 的一个子集 $\{(g,e')\mid g\in G\}$ 是一个子群，它就是 $G\times\{e'\}$．映射 $g\mapsto(g,e')$ 给出了 G 到 $G\times\{e'\}$ 的一个同构，从而 $G\cong G\times\{e'\}$．同理，$G\times G'$ 的一个子集 $\{(e,g')\mid g'\in G'\}$ 也是一个子群，它就是 $\{e\}\times G'$，并且有 $G'\cong\{e\}\times G'$．

类似地，我们可以构造两个以上的群的直积．在笛卡儿积 $G_1\times G_2\times\cdots\times G_s$ 上定义一个二元运算：

$$(x_1,x_2,\cdots,x_s)(y_1,y_2,\cdots,y_s)\xlongequal{\text{def}}(x_1y_1,x_2y_2,\cdots,x_sy_s),\qquad(7)$$

则易验证 $G_1\times G_2\times\cdots\times G_s$ 成为一个群，称它是群 $G_1,G_2,\cdots,G_s$ 的直积，记作 $G_1\times G_2\times\cdots\times G_s$．

例如，域 $\mathbf{Z}_2$ 上的 n 维线性空间 $\mathbf{Z}_2^n$ 的加法群就是 n 个 $\mathbf{Z}_2$ 的直积：$\mathbf{Z}_2\times\mathbf{Z}_2\times\cdots\times\mathbf{Z}_2$．这是因为 $\mathbf{Z}_2^n$ 中的加法的定义为

$$(a_1,a_2,\cdots,a_n)+(b_1,b_2,\cdots,b_n)\xlongequal{\text{def}}(a_1+b_1,a_2+b_2,\cdots,a_n+b_n).\qquad(8)$$

从而 $\mathbf{Z}_2^n$ 的加法群是 n 个 $\mathbf{Z}_2$ 的直积．

群的直积是用小群构造大群的一种最简单的方法．例如上面用 2 阶循环群 $\mathbf{Z}_2$ 与自身的直积构造了一个 4 阶非循环的 abel 群：$\mathbf{Z}_2\times\mathbf{Z}_2$．

我们常常要用 m 阶循环群 $\mathbf{Z}_m$ 与 n 阶循环群 $\mathbf{Z}_n$ 的直积构造一个 mn 阶 abel 群：$\mathbf{Z}_m\times\mathbf{Z}_n$．它有没有可能仍是循环群？下面仔细分析一

下.

$\mathbf{Z}_m$ 是由 $\bar{1}$ 生成的 m 阶循环群,因此 $\bar{1}$ 是 m 阶元. 由于 $\mathbf{Z}_m$ 到 $\mathbf{Z}_m \times \mathbf{Z}_n$ 的一个子群 $\{(\bar{a},\bar{0}) \mid \bar{a} \in \mathbf{Z}_m\}$ 有一个同构映射: $\bar{a} \mapsto (\bar{a},\bar{0})$, 因此在 $\mathbf{Z}_m \times \mathbf{Z}_n$ 中, $(\bar{1},\bar{0})$ 是 m 阶元. 同理 $(\bar{0},\bar{1})$ 是 n 阶元. 由于

$$(\bar{1},\bar{0}) + (\bar{0},\bar{1}) = (\bar{1},\bar{1}),$$

因此如果 $(m,n) = 1$, 则据 §2 的命题 4 得, $(\bar{1},\bar{1})$ 阶是 mn, 从而 $\mathbf{Z}_m \times \mathbf{Z}_n$ 是由 $(\bar{1},\bar{1})$ 生成的 mn 阶循环群. 如果 $(m,n) = d \neq 1$, 设 $m = m'd$, $n = n'd$. 则对于任意 $(\bar{a},\bar{b}) \in \mathbf{Z}_m \times \mathbf{Z}_n$, 有

$$\begin{aligned} m'dn'(\bar{a},\bar{b}) &= (m'dn'\bar{a}, m'dn'\bar{b}) \\ &= (n'm\bar{a}, m'n\bar{b}) \\ &= (\bar{0},\bar{0}), \end{aligned} \tag{9}$$

从而 $(\bar{a},\bar{b})$ 的阶是 $m'dn'$ 的因子. 由于 $m'dn' < mn$, 因此 $(\bar{a},\bar{b})$ 的阶小于 mn. 从而 $\mathbf{Z}_m \times \mathbf{Z}_n$ 不是循环群. 综上所述, 得

命题 3 $\mathbf{Z}_m \times \mathbf{Z}_n$ 是循环群当且仅当 $(m,n) = 1$. 从而 $\mathbf{Z}_m \times \mathbf{Z}_n \cong \mathbf{Z}_{mn}$ 当且仅当 $(m,n) = 1$. □

命题 3 使我们能识别 $\mathbf{Z}_m \times \mathbf{Z}_n$ 是否同构于 $\mathbf{Z}_{mn}$.

从以上的例子看到, 两个群 G 与 G' 的直积 $G \times G'$, 其中 G 与 G' 可能是不同的群, 例如 $\mathbf{Z}_m$ 与 $\mathbf{Z}_n$, 其中 $m \neq n$; 也可能是同一个群, 例如 $\mathbf{Z}_2$ 与自身; 还可能是一个群的两个子群, 例如, SO_3 与 $\{I, -I\}$ 可以构造直积, 而它们都是 O_3 的子群. 我们来探讨 $SO_3 \times \{I, -I\}$ 与 O_3 有什么关系.

例 1 $O_3 \cong SO_3 \times \{I, -I\}$.

证明 令 $\sigma: SO_3 \times \{I, -I\} \longrightarrow O_3$,

$$(A, U) \longmapsto AU.$$

显然 σ 是映射, 现在来证 σ 是单射. 设

$$\sigma(A, U) = \sigma(B, W),$$

则 $AU = BW$, 从而 $B^{-1}A = WU^{-1} \in SO_3 \cap \{I, -I\}$, 由于 $-I \mid$

$(-1)^3|I| = -1$,因此 $-I \notin SO_3$,从而

$$SO_3 \cap \{I, -I\} = \{I\}.$$

于是 $B^{-1}A = WU^{-1} = I$.由此得出,$A = B$,$U = W$,即 $(A, U) = (B, W)$.因此 σ 是单射.

下面来证 σ 是满射.任取 $T \in O_3$.如果 $|T| = 1$,则 $T \in SO_3$,从而 $T = TI = \sigma(T, I)$.如果 $|T| = -1$,则 $|T(-I)| = 1$.记 $\tilde{T} = T(-I)$,则 $\tilde{T} \in SO_3$,从而 $T = \tilde{T}(-I) = \sigma(\tilde{T}, -I)$.因此 σ 是满射.

下面来证 σ 保持运算.任取 $(A, U), (B, W) \in SO_3 \times \{I, -I\}$.我们有

$$\begin{aligned}\sigma[(A, U)(B, W)] &= \sigma(AB, UW) = (AB)(UW) \\ &= (AU)(BW) = \sigma(A, U)\sigma(B, W)\end{aligned} \quad (10)$$

因此 σ 是同构映射,从而 $SO_3 \times \{I, -I\} \cong O_3$. □

在例 1 的证明过程中我们看到:O_3 的每一个元素 T 可以表示成 $T = TI$ 或 $T = \tilde{T}(-I)$,因此

$$O_3 = SO_3\{I, -I\};$$

这保证了 σ 是满射.我们还看到:

$$SO_3 \cap \{I, -I\} = \{I\},$$

这保证了 σ 是单射.我们还看到:SO_3 的每个元素与 $\{I, -I\}$ 的每个元素可交换,这保证了 σ 保持运算.

由例 1 受到启发,我们猜想有下述结论:

定理 4 设 G 是一个群,H, K 是 G 的两个子群.如果

(i) $G = HK \xlongequal{\text{def}} \{hk \mid h \in H, k \in K\}$;

(ii) $H \cap K = \{e\}$;

(iii) H 中每个元素与 K 中每个元素可交换,

则

$$G \cong H \times K.$$

证明 令 $\sigma: H\times K \to G$
$(h,k)\longmapsto hk.$

由于 $G=HK$，因此 G 中每个元素 g 可表示成 $g=hk$，对于某个 $h\in H,k\in K$，从而 $\sigma(h,k)=hk=g$. 因此 σ 是满射. 下面证 σ 是单射. 如果 $\sigma(h_1,k_1)=\sigma(h_2,k_2)$，则 $h_1k_1=h_2k_2$，从而 $h_2^{-1}h_1=k_2k_1^{-1}\in H\cap K$. 由于 $H\cap K=\{e\}$，因此 $h_2^{-1}h_1=k_2k_1^{-1}=e$. 从而 $h_1=h_2,k_1=k_2$. 即 $(h_1,k_1)=(h_2,k_2)$. 因此 σ 是单射. 下面证 σ 保持运算：

$$\sigma[(h_1,k_1)(h_2,k_2)]=\sigma(h_1h_2,k_1k_2)=(h_1h_2)(k_1k_2).$$

由于条件(iii)，因此

$$(h_1h_2)(k_1k_2)=(h_1k_1)(h_2k_2)=\sigma(h_1k_1)\sigma(h_2k_2).$$

从而 σ 保持运算. 综上述得，$H\times K\cong G$. □

设 H,K 是群 G 的两个子群，如果 $G\cong H\times K$，则称 G 是子群 H 与 K 的**内直积**(internal direct product)，习惯上就记作 $G=H\times K$.

注意光是 $G=HK$ 不能保证 G 是子群 H 与 K 的内直积，还必须满足定理 4 中的条件(ii) 和(iii)，才能保证 G 是 H 与 K 的内直积. 条件(ii)：$H\cap K=\{e\}$ 保证了 G 中每个元素 g 表示成 $g=hk$ 的方式唯一. 条件(iii) 保证了 G 中任意两个元素 $g_1=h_1k_1$ 与 $g_2=h_2k_2$ 相乘时，有

$$g_1g_2=(h_1h_2)(k_1k_2).$$

即把 h_1 与 h_2 相乘，k_1 与 k_2 相乘，然后求它们的乘积.

当群 G 的运算记成加法时，如果 G 是它的子群 H 与 K 的内直积，则称 G 是 H 与 K 的**内直和**(internal direct sum)，习惯上记作 $G=H\oplus K$. 注意此时 G 的每个元素 g 可唯一地表示成 $g=h+k$，对于某个 $h\in H,k\in K$.

可以把定理 4 推广到群 G 的多个子群的情形：

定理 5　设 G 是一个群，运算记成加法，$H_1, H_2, \cdots, H_s$ 是 G 的子群，如果

(i) $G = H_1 + H_2 + \cdots + H_s \xlongequal{\text{def}} \{h_1 + h_2 + \cdots + h_s \mid h_i \in H_i, 1 \leqslant i \leqslant s\}$；

(ii) $H_i \cap \left(\sum_{j \neq i} H_j\right) = \{e\}, i = 1, 2, \cdots, s$；

(iii) H_i 的每个元素与 H_j 的每个元素可交换，其中 $i \neq j, 1 \leqslant i, j \leqslant s$.

则
$$G \cong H_1 \oplus H_2 \oplus \cdots \oplus H_s.$$
此时称 G 是子群 $H_1, H_2, \cdots, H_s$ 的内直和，习惯上记作
$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_s.$$
定理 5 的证明方法类似于定理 4 的证法，此处从略.

习题 1.3

1. 证明实数加群 $\mathbf{R}$ 与正实数乘法群 $\mathbf{R}^+$ 同构.

2. 在 $\mathbf{Z}_9$ 的单位群 $U(\mathbf{Z}_9)$ 中，$\bar{2}$ 的阶是多少？$U(\mathbf{Z}_9)$ 与 $\mathbf{Z}_6$ 的加法群同构吗？

3. $U(\mathbf{Z}_8)$ 与 Klein 群 $\mathbf{Z}_2 \times \mathbf{Z}_2$ 同构吗？

4. 习题 1.2 的第 4 题中，正方形棋盘的对称(性)群 G 与 A_4 的子群 $K = \{(1), (12)(34), (13)(24), (14)(23)\}$ 同构吗？

*5. 证明：$D_3 \cong S_3$.

6. 设 G 是一个群. 证明：映射 $\sigma: x \mapsto x^{-1}$ 是 G 到 G 的同构映射当且仅当 G 是 abel 群.

7. 正四面体的旋转对称(性)群 G_1，正十二棱锥的旋转对称(性)群 G_2、正六边形的对称(性)群 D_6 都是 12 阶群，这三个群彼此同构吗？

8. 证明：$\mathbf{Z}_3 \times V \cong \mathbf{Z}_2 \times \mathbf{Z}_6$，其中 V 是 Klein 群.

9．下列四个 24 阶 abel 群中，哪些是彼此同构的？

$$\mathbf{Z}_{24}, \quad \mathbf{Z}_{12}\times\mathbf{Z}_2, \quad \mathbf{Z}_6\times\mathbf{Z}_4, \quad \mathbf{Z}_2\times\mathbf{Z}_4\times\mathbf{Z}_3.$$

*10．下列三个 24 阶非交换群中，有同构的吗？

$$D_{12}, \quad D_4\times\mathbf{Z}_3 \quad A_4\times\mathbf{Z}_2.$$

*11．证明：当 n 是奇数时，$D_{2n}\cong D_n\times\mathbf{Z}_2$.

*12．设 n 为奇数，证明：

(1) $O_n\cong SO_n\times\{I,-I\}$;

(2) $O_n\cong SO_n\times\mathbf{Z}_2$.

§4 群的同态，正规子群，商群，可解群

图 1－5 是一个物体的三视图（依次为从上往下看，从前往后看，从右往左看）．你能说出这个物体的形状吗？

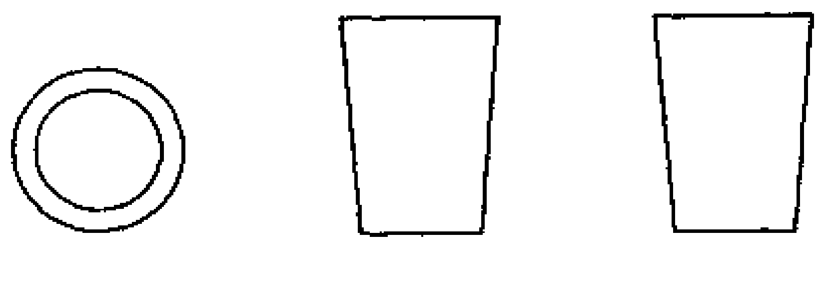


图 1－5

这是一个圆台形状的物体，例如茶杯．一个物体的三视图就是把它分别投影到空间直角坐标系 $Oxyz$ 的三个坐标平面上，然后从它的三个投影了解物体的形状和大小．投影是几何空间 V 上的一个线性变换．从而它是 V 的加法群到自身的保持运算的映射．从日常生活中的例子看到，这类映射是相当有用的．为此我们引出下述重要概念：

定义 1 设 G 和 G' 是两个群，如果 G 到 G' 有一个映射 σ，使得对于 G 中任意两个元素 a,b 都有

$$\sigma(ab) = \sigma(a)\sigma(b), \tag{1}$$

则称 σ 是群 G 到 G' 的一个**同态映射**,简称为**同态**(homomorphism).

群 G 到 G' 的同态映射 σ 只比同构映射少了"σ 是双射"这个条件,它们都是保持运算的映射.因此在同构映射的性质中,凡是没有用到"σ 是双射"这个条件的,对于同态映射也成立.于是我们有下述结论:

命题 1 设 σ 是群 G 到 G' 的一个同态,则

(1) σ 把 G 的单位元 e 映成 G' 的单位元 e';

(2) $\sigma(a^{-1}) = \sigma(a)^{-1}, \forall a \in G$;

(3) G 的子群 H 在 σ 下的像 $\sigma(H)$ 是 G' 的子群;

(4) G 在 σ 下的像 $\mathrm{Im}\sigma$ 是 G' 的子群,称 $\mathrm{Im}\sigma$ 是同态 σ 的**像**(image). □

注意:对于群 G 到 G' 的一个同态 σ,由于

$$a^n = e \Longrightarrow \sigma(a)^n = e',$$

因此 σ 有可能把 G 的无限阶元 a 映成 G' 的有限阶元;如果 a 是 G 里的 n 阶元,则 $\sigma(a)$ 的阶是 n 的一个因子.

设 σ 是群 G 到 G' 的一个同态,如果 σ 是满射,则称 σ 是**满同态**(epimorphism);如果 σ 是单射,则称 σ 是**单同态**(monomorphism),或者**嵌入**(embedding).

显然,群 G 到 G' 的同态 σ 是满同态当且仅当 $\mathrm{Im}\sigma = G'$. σ 是单同态的特征是什么?为此需引进下述概念:

定义 2 设 σ 是群 G 到 G' 的一个同态,则 G' 的单位元 e' 的原像集称为 σ 的**核**(kernel),记作 $\mathrm{Ker}\,\sigma$. 即

$$\mathrm{Ker}\,\sigma \xlongequal{\text{def}} \{a \in G \mid \sigma(a) = e'\}. \tag{2}$$

事实 1 群 G 到 G' 的同态 σ 的核 $\mathrm{Ker}\,\sigma$ 是 G 的一个子群.

证明 由于 $\sigma(e) = e'$,因此 $e \in \mathrm{Ker}\sigma$.

任取 $a, b \in \mathrm{Ker}\sigma$,则

$$\sigma(ab^{-1}) = \sigma(a)\sigma(b)^{-1} = e'e'^{-1} = e',$$

因此 $ab^{-1} \in \mathrm{Ker}\sigma$. 从而 $\mathrm{Ker}\sigma < G$. □

事实 2 群 G 到 G' 的同态 σ 是单同态当且仅当 $\mathrm{Ker}\sigma = \{e\}$.

证明 必要性是显然的. 我们来证充分性. 设 $a, b \in G$ 使得 $\sigma(a) = \sigma(b)$. 则 $\sigma(a)\sigma(b)^{-1} = e'$. 从而 $\sigma(ab^{-1}) = e'$. 因此 $ab^{-1} \in \mathrm{Ker}\sigma$. 由于 $\mathrm{Ker}\sigma = \{e\}$, 因此 $ab^{-1} = e$, 从而 $a = b$. 这表明 σ 是单射. □

例 1 下述映射 σ 是不是群 $\mathbf{Z}$ 到 $\mathbf{Z}_m$ 的一个同态? σ 的像 $\mathrm{Im}\sigma$ 是什么? σ 的核 $\mathrm{Ker}\sigma$ 是什么?

$$\sigma: \mathbf{Z} \longrightarrow \mathbf{Z}_m$$
$$a \longmapsto \overline{a}.$$

解 由于对于任意 $a, b \in \mathbf{Z}$, 都有

$$\sigma(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \sigma(a) + \sigma(b),$$

因此 σ 是群 $\mathbf{Z}$ 到 $\mathbf{Z}_m$ 的一个同态, 显然 σ 是满射. 因此 $\mathrm{Im}\sigma = \mathbf{Z}_m$. 由于

$$a \in \mathrm{Ker}\sigma \Longleftrightarrow \overline{a} = \overline{0}$$
$$\Longleftrightarrow a = ml, \text{对某个 } l \in \mathbf{Z},$$

因此 $\mathrm{Ker}\sigma = \{ml \mid l \in \mathbf{Z}\}$. 令

$$m\mathbf{Z} \xlongequal{\text{def}} \{ml \mid l \in \mathbf{Z}\}. \tag{3}$$

则 $$\mathrm{Ker}\sigma = m\mathbf{Z}.$$

从例 1 看出, 任给一个正整数 m, 都有 m 阶循环群 $\mathbf{Z}_m$ 是无限循环群 $\mathbf{Z}$ 的一个同态像.

从例 1 还可看出, $\mathbf{Z}$ 里的无限阶元素 1 在同态 σ 下的像 $\overline{1}$ 是 $\mathbf{Z}_m$ 里的 m 阶元.

例 2 下述对应法则 τ 是不是 n 级正交群 O_n 到 2 次单位根群 U_2 的一个同态? $\mathrm{Im}\tau$, $\mathrm{Ker}\tau$ 分别是什么?

$$\tau: O_n \longrightarrow U_2$$

$$T \longmapsto |T|.$$

解 由于正交矩阵的行列式为 1 或 -1,因此 τ 是 O_n 到 U_2 的一个映射.由于对于任意 $T_1, T_2 \in O_n$,都有

$$\tau(T_1T_2) = |T_1T_2| = |T_1||T_2| = \tau(T_1)\tau(T_2),$$

因此 τ 是群 O_n 到 U_2 的一个同态.显然 τ 是满射,因此 $\mathrm{Im}\tau = U_2$.由于

$$T \in \mathrm{Ker}\tau \Longleftrightarrow |T| = 1 \Longleftrightarrow T \in SO_n,$$

因此 $\mathrm{Ker}\tau = SO_n$.

我们来分析例 2 中的 $\mathrm{Ker}\tau$(即 SO_n)有什么性质.记 $K = \mathrm{Ker}\tau$,由于相似的矩阵有相同的行列式,因此对于任意给定的 $T \in O_n$,任取 $A \in SO_n$(即,K),有

$$|TAT^{-1}| = |(T^{-1})^{-1}A(T^{-1})| = |A| = 1.$$

从而 $TAT^{-1} \in K$.令

$$TKT^{-1} \xlongequal{\text{def}} \{TAT^{-1} \mid A \in K\} \tag{4}$$

则上述表明

$$TKT^{-1} \subseteq K, \quad \forall\, T \in O_n \tag{5}$$

从而有 $$T^{-1}KT \subseteq K, \quad \forall\, T \in O_n.$$

于是对于任意 $B \in K$,有

$$B = T(T^{-1}BT)T^{-1} \in TKT^{-1},$$

从而有 $$K \subseteq TKT^{-1} \tag{6}$$

从(5)、(6)式得出

$$TKT^{-1} = K, \quad \forall\, T \in O_n. \tag{7}$$

(7)式就是 $\mathrm{Ker}\tau$ 具有的性质.

一般地,我们有

命题 2 设 σ 是群 G 到 G' 的一个同态,记 $K = \mathrm{Ker}\sigma$,则

$$gKg^{-1} = K, \quad \forall\, g \in G. \tag{8}$$

证明 任意给定 $g \in G$，任取 $x \in K$，有

$$\sigma(gxg^{-1}) = \sigma(g)\sigma(x)\sigma(g)^{-1} = \sigma(g)e'\sigma(g)^{-1} = e'.$$

因此 $gxg^{-1} \in K$，从而 $gKg^{-1} \subseteq K$. 于是也有 $g^{-1}Kg \subseteq K$. 从而对任意 $y \in K$，有

$$y = g(g^{-1}yg)g^{-1} \in gKg^{-1}.$$

于是 $K \subseteq gKg^{-1}$. 综上述得，

$$gKg^{-1} = K, \quad \forall g \in G.$$

□

从同态 σ 的核 $\mathrm{Ker}\sigma$ 具有的上述性质受到启发，我们抽象出下述重要概念：

定义 3 群 G 的一个子群 N 如果满足

$$gNg^{-1} = N, \quad \forall g \in G, \tag{9}$$

则称 N 是 G 的一个**正规子群**(normal subgroup)，记作 $N \lhd G$.

从命题 2 立即得到，设 σ 是群 G 到 G' 的一个同态，则

$$\mathrm{Ker}\sigma \lhd G. \tag{10}$$

设 H 是群 G 的一个子群. 容易验证，对于任意 $g \in G$，有 gHg^{-1} 也是 G 的一个子群，称 gHg^{-1} 是 H 的一个**共轭子群**(conjugate subgroup). 从定义 3 立即得出：

事实 3 群 G 的一个子群 N 是 G 的正规子群当且仅当 N 的所有共轭子群都等于 N 自身. □

显然，$\{e\}$ 和 G 都是群 G 的正规子群，称它们是**平凡的正规子群**. G 的其余的正规子群（如果有的话）称为**非平凡的**(non-trivial).

正规子群的特征还可以用下述命题来刻画：

命题 3 群 G 的一个子群 H 是 G 的正规子群当且仅当对于 G 中每一个元素 a，都有 $aH = Ha$.

证明 必要性. 设 $H \lhd G$. 任取 $a \in G$，有 $aHa^{-1} = H$. 于是对于任意 $h \in H$，有 $aha^{-1} \in H$，从而有

$$ah = (aha^{-1})a \in Ha.$$

因此 $aH \subseteq Ha$. 类似地可证, $Ha \subseteq aH$. 因此 $aH = Ha$.

充分性. 任意给定 $g \in G$, 任取 $h \in H$, 由于 $gH = Hg$, 因此存在 $h' \in H$, 使得 $gh = h'g$, 从而 $ghg^{-1} = h' \in H$. 因此 $gHg^{-1} \subseteq H$. 于是也有 $g^{-1}Hg \subseteq H$. 从而对于任意 $y \in H$, 有 $y = g(g^{-1}yg)g^{-1} \in gHg^{-1}$. 因此 $H \subseteq gHg^{-1}$. 综上述得, $gHg^{-1} = H, \forall g \in G$. 这证明了 $H \lhd G$. □

从命题 3 的充分性的证明过程看出, 在证明群 G 的一个子群 H 是 G 的正规子群时, 可采用下述方法:

命题 4 设 H 是群 G 的一个子群, 如果对于任意给定的 $g \in G$, 任取 $h \in H$, 都有 $ghg^{-1} \in H$, 则 H 是 G 的正规子群. □

从命题 3 立即看出, abel 群的每一个子群都是正规子群.

从命题 3 还可以得出:

推论 5 如果 H 是群 G 的指数为 2 的子群, 则 H 是 G 的正规子群.

证明 任取 $a \in G$, 若 $a \in H$, 则 $aH = H = Ha$. 下面设 $a \notin H$. 此时有

$$G = H \cup aH, \quad G = H \cup Ha.$$

由此得出, $aH = Ha$. 从而 $H \lhd G$. □

例如, 当 $n > 1$ 时, 由于 $[S_n : A_n] = 2$, 因此 $A_n \lhd S_n$.

例 3 证明 A_4 的 4 阶子群 V 是 A_4 的正规子群, 也是 S_4 的正规子群.

证明 A_4 的 4 阶子群为

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

S_4 中的置换 σ, 如果 σ 的轮换表示是两个不相交的对换的乘积, 则 $\sigma \in V$. 于是对于任意给定的 $\tau \in S_4$, 任取 $(a_1a_2)(a_3a_4) \in V$, 我们有

$$\tau(a_1a_2)(a_3a_4)\tau^{-1} = [\tau(a_1a_2)\tau^{-1}][\tau(a_3a_4)\tau^{-1}]$$
$$= (\tau(a_1) \quad \tau(a_2))(\tau(a_3) \quad \tau(a_4)) \in V.$$

又 $\tau e \tau^{-1} = e \in V$. 因此 $V \lhd S_4$. 从而也有 $V \lhd A_4$. □

正规子群在研究群的结构中起着十分重要的作用.

设 N 是群 G 的一个正规子群，则对于所有的 $a \in G$，有 $aN = Na$. 从而 $(G/N)_l = (G/N)_r$. 于是可以把 G 关于正规子群 N 的左（右）商集就称为**商集**(quotient set)，记作 G/N. 在商集 G/N 中能不能定义一个二元运算？由于 G/N 中的元素是 N 的左陪集（或者说右陪集），它们都是群 G 的子集，所以我们首先来规定群 G 的两个子集 A 与 B 的乘法：

$$AB \xlongequal{\text{def}} \{ab \mid a \in A,\ b \in B\}. \tag{11}$$

显然，群 G 的子集的乘法满足结合律：

$$(AB)C = A(BC). \tag{12}$$

如果 $A = \{a\}$，则把 AB 简记成 aB.

现在任取正规子群 N 的两个左陪集 aN, bN，有

$$\begin{aligned}(aN)(bN) &= a(Nb)N = a(bN)N = (abN)N \\ &= ab(NN) = abN.\end{aligned} \tag{13}$$

(13) 式表明，正规子群 N 的任意两个左陪集 aN 与 bN 的乘积是左陪集 abN，因此我们可以在商集 G/N 中定义一个二元运算如下：

$$(aN)(bN) = abN. \tag{14}$$

从(14)式看出，两个陪集相乘实际上就归结为它们的代表相乘，因此容易看出，(14)式定义的乘法满足结合律. 由于对于所有的 $aN \in G/N$，有

$$N(aN) = (eN)(aN) = eaN = aN,$$

$$(aN)N = aN,$$

因此 N 是 G/N 的单位元素，由于

$$(aN)(a^{-1}N) = aa^{-1}N = eN = N,$$

因此 G/N 中每个元素 aN 有逆元 $a^{-1}N$，从而商集 G/N 成为一个群，称它为群 G 对于正规子群 N 的**商群**(quotient group).

思考：如果群 G 的子群 H 不是正规子群，那么 H 的任意两个左陪集 aH 与 bH 的乘积还是 H 的左陪集吗？左商集 $(G/H)_l$ 能够成为一个群吗？

事实 4　设 G 是一个有限群，$N \lhd G$，则商群 G/N 的阶等于 $\frac{|G|}{|N|}$．□

群 G 与它对于正规子群 N 的商群 G/N 之间有什么关系呢？显然，商群 G/N 的元素已经不是 G 的元素，但是 G 与 G/N 仍有密切的关系．下面的命题 6 告诉我们，商群 G/N 是群 G 的一个同态像．

命题 6　设 N 是群 G 的一个正规子群．令

$$\begin{aligned}\pi:\ G &\longrightarrow G/N\\ a &\longmapsto aN,\end{aligned} \tag{15}$$

则 π 是群 G 到商群 G/N 的一个满同态，并且 $\mathrm{Ker}\pi = N$．

证明　对于 G 中任意两个元素 a，b，有

$$\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b),$$

因此 π 是群 G 到 G/N 的一个同态．显然 π 是满射．由于

$$a \in \mathrm{Ker}\pi \Longleftrightarrow \pi(a) = N \Longleftrightarrow aN = N \Longleftrightarrow a \in N,$$

因此 $\mathrm{Ker}\pi = N$．□

命题 6 中定义的同态 $\pi: a \mapsto aN$，称为**自然同态**(natural homomorphism)，或者**标准同态**(canonical homomorphism)．命题 6 告诉我们，商群 G/N 是群 G 在自然同态下的像；还告诉我们，正规子群 N 是自然同态的核．而(10)式告诉我们，群 G 到 G' 的任一同态 σ 的核 $\mathrm{Ker}\sigma$ 是 G 的正规子群．这样我们对正规子群与同态核之间的密切关系就了如指掌了．类似地考虑，既然商群 G/N 是群 G 的一个同态像，那么反过来，群 G 的任一同态像与 G 关于同态核的商群之间有什么关系？下面的定理 7 回答了这一问题．

定理 7(群同态基本定理)　设 σ 是群 G 到 G' 的一个同态，则同态像同构于商群 $G/\mathrm{Ker}\sigma$，即

$$G/\mathrm{Ker}\sigma \cong \mathrm{Im}\sigma. \tag{16}$$

证明 记 $N=\mathrm{Ker}\sigma$. 则 $N \triangleleft G$,从而有商群 G/N. 令

$$\begin{aligned}\psi:\ G/N &\longrightarrow \mathrm{Im}\sigma\\ aN &\longmapsto \sigma(a).\end{aligned} \tag{17}$$

由于

$$\begin{aligned} aN = bN &\Longleftrightarrow b^{-1}a \in N\\ &\Longleftrightarrow \sigma(b^{-1}a) = e'\\ &\Longleftrightarrow \sigma(a) = \sigma(b),\end{aligned}$$

因此 ψ 是 G/N 到 $\mathrm{Im}\sigma$ 的一个映射,并且 ψ 是单射. 显然 ψ 是满射. 对于任意 $aN, bN \in G/N$,有

$$\begin{aligned}\psi[(aN)(bN)] &= \psi(abN) = \sigma(ab) = \sigma(a)\sigma(b)\\ &= \psi(aN)\psi(bN).\end{aligned}$$

因此 ψ 是 G/N 到 $\mathrm{Im}\sigma$ 的一个同构,从而

$$G/N \cong \mathrm{Im}\sigma. \qquad \square$$

例 1 中指出,群 $\mathbf{Z}$ 到 $\mathbf{Z}_m$ 有一个满同态 σ,且 $\mathrm{Ker}\sigma = m\mathbf{Z}$. 于是据群同态基本定理,得

$$\mathbf{Z}/m\mathbf{Z} \cong \mathbf{Z}_m. \tag{18}$$

利用群同态基本定理可以推导出一些群是同构的. 首先要建立一个合适的映射 σ,证明它是满同态;然后去求同态的核 $\mathrm{Ker}\sigma$,最后据群同态基本定理得,同态像同构于商群. 下面是用这种方法得到的两个重要的同构定理.

定理 8(第一同构定理) 设 G 是群, $H < G$, $N \triangleleft G$,则

(1) $HN < G$;

(2) $H \cap N \triangleleft H$,且 $H/H\cap N \cong HN/N$.

证明 (1) 显然 HN 是非空集,任取 $h_1n_1, h_2n_2 \in HN$,有

$$\begin{aligned}(h_1n_1)(h_2n_2)^{-1} &= h_1n_1n_2^{-1}h_2^{-1}\\ &= (h_1h_2^{-1})[h_2(n_1n_2)^{-1}h_2^{-1}] \in HN.\end{aligned}$$

因此 $HN < G$.

(2) 由于 $N \lhd G$，因此 $N \lhd HN$，令

$$\sigma: H \longrightarrow HN/N$$
$$h \longmapsto hN.$$

在 HN/N 中任取 $(hn)N = hN$，则 $\sigma(h) = hN = (hn)N$. 因此 σ 是满射. 对于任意 $h_1, h_2 \in H$，有

$$\sigma(h_1h_2) = h_1h_2N = (h_1N)(h_2N)$$
$$= \sigma(h_1)\sigma(h_2).$$

因此 σ 是 H 到 HN/N 的一个满同态. 我们有

$$h \in \mathrm{Ker}\sigma \Longleftrightarrow hN = N \Longleftrightarrow h \in H \cap N,$$

因此 $\mathrm{Ker}\sigma = H \cap N$，从而 $H \cap N \lhd H$. 据群同态基本定理，得

$$H/H \cap N \cong HN/N. \quad \square$$

注：类似地可证明，若 $H < G, N \lhd G$，则

(1) $NH < G$;

(2) $H/H \cap N \cong NH/N$.

定理 9(第二同构定理) 设 G 是一个群，$H \lhd G, N \lhd G$，且 $N \subseteq H$，则 $H/N \lhd G/N$，且

$$(G/N)/(H/N) \cong G/H.$$

证明 令

$$\sigma: G/N \longrightarrow G/H$$
$$aN \longmapsto aH.$$

如果 $aN = bN$，则 $b^{-1}a \in N$. 由于 $N \subseteq H$，因此 $b^{-1}a \in H$，从而 $aH = bH$. 这表明 σ 是一个映射. 显然 σ 是满射. 对于任意 $aN, bN \in G/N$，有

$$\sigma[(aN)(bN)] = \sigma(abN) = abH$$
$$= (aH)(bH) = \sigma(aN)\sigma(bN).$$

因此 σ 是 G/N 到 G/H 的一个满同态. 我们有

$$aN \in \mathrm{Ker}\sigma \Longleftrightarrow aH = H \Longleftrightarrow a \in H$$

$$\Longleftrightarrow aN \in H/N,$$

因此 $\mathrm{Ker}\sigma = H/N$. 从而 $H/N \lhd G/N$. 据群同态基本定理,得

$$(G/N)/(H/N) \cong G/H.$$ □

如同从一个茶杯在三个不同方向上的投影可以了解茶杯的形状和大小一样,对于群 G,我们可以从它的不同的同态像去了解 G 的结构. 而从群同态基本定理知道,群 G 的每一个同态像都同构于 G 对于同态核的商群. 又同态核是 G 的正规子群,反之亦然. 因此只要掌握了群 G 的所有正规子群,那么就把握了群 G 的所有同态像,从而可了解群 G 的结构. 这就是为什么说正规子群在研究群的结构中起着十分重要的作用的缘故.

如果一个群 G 只有平凡的正规子群,则称 G 是**单群**(simple group).

由于单群没有非平凡的正规子群,因此单群的同态像或者同构于 $\{e\}$,或者同构于 G. 通俗地说,单群是"抱成一团"的群,无法把它"拆开". 于是单群是群论的基本构件. 犹如砖是砖房的基本构件,素数是整数理论的基本构件一样.

能不能找出所有的单群?或者找出所有的有限单群?

abel 群的每一个子群都是正规子群,因此如果 abel 群 G 是单群,则 G 的子群只有两个:$\{e\}$ 和 G,从而当 $a \neq e$ 时,$\langle a \rangle = G$. 由于无限循环群和合数阶循环群都有非平凡的子群,因此 $G = \langle a \rangle$ 必为素数阶循环群. 反之,如果 G 是素数阶循环群,则显然 G 是单群. 这样我们证明了:

abel 群 G 是单群当且仅当 G 是素数阶循环群.

非 abel 群中哪些是单群?我们用排除法,先把非 abel 群中不是单群的找出来,排除掉;再从剩下的群中去找单群.

下面我们将介绍一类非 abel 群,它们都不是单群,并且它们与 abel 群有着密切的联系. 让我们先看一个例子.

交错群 A_4 有正规子群 V:

$$V = \{e,(12)(34),(13)(24),(14)(23)\},$$

因此 A_4 不是单群．由于 $|A_4/V| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3$，因此商群 A_4/V 是 3 阶循环群，即 abel 群．

从 A_4 这个例子受到启发，对于任一群 G，我们想找它的一个正规子群 N，使得商群 G/N 是 abel 群．由于商群 G/N 是群 G 的一个同态像，正规子群 N 是同态核，因此找 G 的正规子群 N，使得商群 G/N 为 abel 群，就需要去找群 G 到某一个群 G' 的一个同态 σ，使得同态像 $\mathrm{Im}\sigma$ 为 abel 群．现在我们来分析同态像 $\mathrm{Im}\sigma$ 为 abel 群的条件是什么．

设 σ 是群 G 到 $\tilde{G}$ 的一个同态，则

$$\begin{aligned}
&\mathrm{Im}\sigma \text{ 为 abel 群} \\
\Longleftrightarrow\ &\sigma(x)\sigma(y) = \sigma(y)\sigma(x),\ \forall\, \sigma(x),\sigma(y) \in \mathrm{Im}\sigma \\
\Longleftrightarrow\ &\sigma(xyx^{-1}y^{-1}) = e',\ \forall\, x,y \in G \\
\Longleftrightarrow\ &xyx^{-1}y^{-1} \in \mathrm{Ker}\sigma,\ \forall\, x,y \in G \\
\Longleftrightarrow\ &\{xyx^{-1}y^{-1} \mid x,y \in G\} \subseteq \mathrm{Ker}\sigma
\end{aligned} \tag{19}$$

我们把 $xyx^{-1}y^{-1}$ 称为 x 与 y 的**换位子**(commutator)，记作 $[x,y]$．显然

$$xy = yx \Longleftrightarrow xyx^{-1}y^{-1} = e. \tag{20}$$

定义 4 群 G 的所有换位子生成的子群称为 G 的**换位子群**(commutator subgroup)，或者**导群**(derived group)，记作 $[G,G]$ 或者 G'(注意本书也用 G' 表示任意一个群，因此要从上下文区别 G' 是指 G 的换位子群，还是指任意一个群)，即

$$G' = \langle \{xyx^{-1}y^{-1} \mid x,y \in G\} \rangle. \tag{21}$$

显然有

事实 5 群 G 为 abel 群当且仅当 $G' = \{e\}$． □

由此看出，G 的换位子群 G' 刻画了 G 离 abel 群有多远．粗略地说，G' 越大，则 G 离 abel 群越远．

命题 10 群 G 的换位子群 G' 是 G 的一个正规子群.

证明 任意给定 $g \in G$，任取 $z \in G'$，有

$$gzg^{-1}z^{-1} \in G',$$

从而
$$gzg^{-1} = (gzg^{-1}z^{-1})z \in G'.$$

因此
$$G' \lhd G. \qquad \square$$

从(19)式和 G' 的定义得出：

命题 11 设 σ 是群 G 到 $\widetilde{G}$ 的一个同态，则

$$\mathrm{Im}\sigma \text{ 为 abel 群} \Longleftrightarrow G' \subseteq \mathrm{Ker}\sigma. \qquad \square$$

从命题 11 可得出：

定理 12 设 G' 是群 G 的换位子群，$N \lhd G$，则

(1) G/G' 是 abel 群；

(2) G/N 为 abel 群当且仅当 $G' \subseteq N$.

证明 (1) 由于 $G' \lhd G$，因此有商群 G/G'，考虑自然同态 $\pi: G \to G/G'$. 由于 $\mathrm{Im}\pi = G/G'$，$\mathrm{Ker}\pi = G'$，因此据命题 11 得，G/G' 为 abel 群.

(2) 考虑自然同态 $\pi: G \to G/N$. 由于 $\mathrm{Im}\pi = G/N$，$\mathrm{Ker}\pi = N$，因此据命题 11 得

$$G/N \text{ 为 abel 群} \Longleftrightarrow G' \subseteq N. \qquad \square$$

从定理 12 看出，G 的所有 abel 商群中，G/G' 是最大的一个，形成商群 G/G'，称为把 G"abel 化"(abelianise).

例 4 求 A_4 的换位子群.

解 我们已知道，A_4/V 是 abel 群，因此 $A_4' \subseteq V$. 由于

$$(123)[(12)(34)](123)^{-1} = (23)(14),$$

因此 $\langle(12)(34)\rangle$ 不是 A_4 的正规子群. 同理，V 的其余两个 2 阶子群也不是 A_4 的正规子群. 又 A_4 是非交换群，因此 $A_4' \neq \{e\}$. 从而 $A_4' = V$. $\square$

在例 4 中，$A_4' = V$，而 V 是 4 阶 abel 群，因此 $V' = \{e\}$. 于是 A_4

有一个递降的子群列:

$$A_4 \triangleright A_4' \triangleright \{e\}. \tag{22}$$

一般地,设 G 是一个群,我们把 G' 的换位子群记作 $G^{(2)}$,把 $G^{(2)}$ 的换位子群记作 $G^{(3)}$,……,通过逐次求换位子群可得到 G 的一个递降的子群列:

$$G \triangleright G' \triangleright G^{(2)} \triangleright \cdots \triangleright G^{(k-1)} \triangleright G^{(k)} \triangleright \cdots \tag{23}$$

称它为 G 的**导群列**(derived groups series).

如果 G 是有限群,则 G 的导群列只有两种可能:

情形 1 从某一个正整数 k 开始,有

$$G^{(k)} = G^{(k+1)} \neq \{e\}.$$

情形 2 有一个正整数 k,使得 $G^{(k)} = \{e\}$.

定义 5 设 G 是一个群,如果有一个正整数 k,使得 $G^{(k)} = \{e\}$,则称 G 为**可解群**(solvable group);否则,称 G 是**不可解群**.

对于任一 abel 群 G,由于 $G' = \{e\}$,因此 G 是可解群.这表明 abel 群都是可解群.

从(22)式看出,A_4 是可解群.

事实 6 非 abel 的可解群不是单群.

证明 设 G 是非 abel 群的可解群,则 $G' \neq \{e\}$,且 $G' \neq G$(假如 $G' = G$,则通过逐次求导群,到达不了 $\{e\}$,这与 G 是可解群矛盾).因此 G 有非平凡的正规子群 G',从而 G 不是单群. □

事实 6 告诉我们,非 abel 单群只能从不可解群中去寻找,这给寻找非 abel 单群指明了方向.

1962 年,W. Feit 和 J. Thompson 证明了:每一个奇数阶群都是可解群,其证明长达 255 页.这个结果称为 Feit – Thompson 定理,它表明:不可解的有限群必为偶数阶群.从而 Feit – Thompson 定理证明了 Barnside 猜想:有限群中,所有非 abel 单群都是偶数阶群.

找出所有的有限单群的问题称为**有限单群分类问题**,它是在 20 世纪 40 年代初提出的.R. Brauer 是有限单群分类工作的先驱,他从

1940 年左右开始用模特征标理论研究有限单群问题；1942 年他与我国数学家段学复合作完成了 10000 阶以下的单群分类；1954 年又证明了关于对合的中心化子定理，这条定理不仅促使人们发现了很多新的散在单群，而且提供了将任意给定单群纳入所提出的分类范畴的初步方法，因此成为有限单群分类工作的新起点．Brauer 之后的一个重要突破便是上述 Feit – Thompson 定理．经过 40 年的努力，1980 年一部分数学家宣告有限单群分类问题获得解决，全部的有限单群是：

（ⅰ）素数阶循环群；

（ⅱ）$n \geqslant 5$ 的交错群 A_n；

（ⅲ）Lie 型单群（共 16 族）；

（ⅳ）26 个散在单群．

这个结果称为**有限单群分类定理**，它由 500 多篇论文组成，在各种数学杂志上占了约 15000 页版面．这样冗长的证明使不少数学家怀疑其中会有错误．对此，在该定理的最后证明中起重要作用的 M. Aschbacher 评论道：

"一方面，当证明长度增加时，错误的概率也增加了．在分类定理证明中出现错误的概率实际上是 1．但是另一方面，任何单个错误不能被容易地改正的概率是 0．随着时间的推移，我们将会有机会推敲证明，对它的信任度必定会增加．"

（注：上述关于有限单群分类问题的历史和 Aschbacher 的评论，都引自《数学史教程》，李文林著，高等教育出版社和施普林格出版社 2000 年出版，第 353 – 354 页）．

习题 1.4

1．设 f 是实数加法群 $\mathbf{R}$ 到非零复数乘法群 $\mathbf{C}^*$ 的一个映射：$f(x) = e^{2\pi i x}$，$\forall x \in \mathbf{R}$．

(1) 证明 f 是一个同态；

(2) 求 $\mathrm{Ker}f$ 和 $\mathrm{Im}f$.

2. 设 ψ 是非零复数乘法群 $\mathbf{C}^*$ 到自身的一个映射：$\psi(z)=\frac{z}{|z|}$，$\forall z\in\mathbf{C}^*$.

(1) 证明 ψ 是一个同态；

(2) 求 $\mathrm{Ker}\psi$ 和 $\mathrm{Im}\psi$.

3. 设 F 是一个域，σ 是 $GL_n(F)$ 到 F^* 的一个映射：$\sigma(A)=|A|$，$\forall A\in GL_n(F)$.

(1) 证明 σ 是一个同态；

(2) 求 $\mathrm{Ker}\sigma$ 和 $\mathrm{Im}\sigma$；

(3) 证明：$SL_n(F)\lhd GL_n(F)$；

(4) 证明：$GL_n(F)/SL_n(F)\cong F^*$.

4. 设 G 是实数域 $\mathbf{R}$ 上所有一次函数组成的集合，H 是一次项的系数为 1 的所有一次函数组成的集合，证明：

(1) G 对于映射的乘法成一个群；

(2) H 是 G 的正规子群；

(3) $G/H\cong R^*$，其中 R^* 是非零实数的乘法群.

5. 设 C 表示复平面上的单位圆，它对于复数乘法成一个群. 证明：$\mathbf{R}/\mathbf{Z}\cong C$.

6. 设 C 是复平面上的单位圆，证明：

$$\mathbf{C}^*/\mathbf{R}^+\cong C.$$

7. 设 G 和 G' 是两个群，证明：$G\times\{e'\}\lhd G\times G'$，$\{e\}\times G'\lhd G\times G'$，并且

$$G\times G'/G\times\{e'\}\cong G',\quad G\times G'/\{e\}\times G'\cong G.$$

8. 设群 G 是它的子群 H 与 K 的内直积，证明：$H\lhd G$，$K\lhd G$，并且

$$G/H\cong K,\quad G/K\cong H.$$

9. 分别求 D_3, D_4 的换位子群.

*10. 分别求 D_{2m-1}, D_{2m} 的换位子群,其中 $m \geqslant 2$.

11. 求 S_4 的换位子群.

*12. 求 S_n 的换位子群,其中 $n \geqslant 3$.

*13. 证明:当 $n \geqslant 5$ 时,$A_n' = A_n$.

(注:这表明当 $n \geqslant 5$ 时,A_n 是不可解群.再结合第12题知,当 $n \geqslant 5$ 时,S_n 是不可解群.)

14. 写出 S_4 的导群列,由此看出,S_4 是可解群.

*15. 证明:如果置换群 G 含有奇置换,则 G 必有指数为 2 的子群.

*16. 设 σ 是群 G 到群 G' 的一个满同态,记 $K = \mathrm{Ker}\sigma$. 设 $H' < G'$. 令 $\sigma^{-1}(H') \xlongequal{\text{def}} \{g \in G \mid \sigma(g) \in H'\}$. 证明:

(1) $\sigma^{-1}(H') < G$,且 $\sigma^{-1}(H') \supseteq K$;

(2) $H' \mapsto \sigma^{-1}(H')$ 是 G' 的子群集合到 G 的包含 K 的子群集合的一个双射.

*17. 证明:当 $n \geqslant 5$ 时,A_n 是单群.

*18. 设 G 是一个群,$N \lhd G$,$H < G$. 如果

$$G = NH, \text{且 } N \cap H = \{e\},$$

则称 G 可分解成它的正规子群 N 与子群 H 的**半直积**(semidirect product). 证明:如果 G 可分解成正规子群 N 与子群 H 的半直积,则

$$G/N \cong H.$$

*19. 证明:S_n 可分解成 A_n 与 $\langle(12)\rangle$ 的半直积,其中 $n \geqslant 3$.

§5 群在集合上的作用,群的自同构,轨道一稳定子定理

我们已经知道,正四面体的旋转对称(性)群 G 为

$$G = \{I, \sigma_i, \sigma_i^2, \gamma_j \mid 1 \leqslant i \leqslant 4, 1 \leqslant j \leqslant 3\},$$

其中 σ_i 是绕顶点 i 与对面中心的连线转角为 $\frac{2\pi}{3}$ 的旋转，γ_j 是绕一对对棱中点的连线转角为 π 的旋转，$1 \leqslant i \leqslant 4, 1 \leqslant j \leqslant 3$. 如图 1－6 所示.

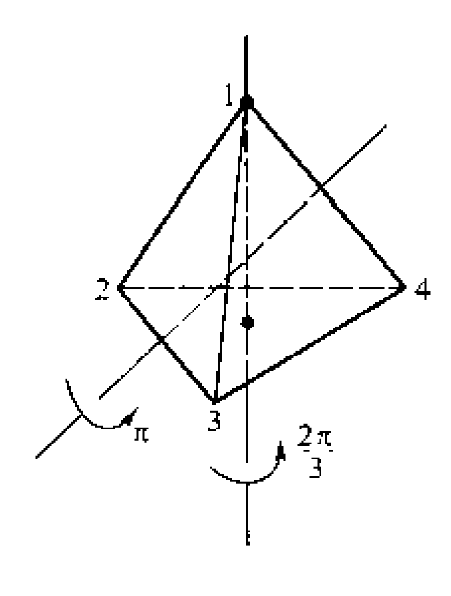


图 1－6

正四面体的 4 个顶点组成的集合记作 Ω，即 $\Omega = \{1,2,3,4\}$. 显然群 G 的每一个元素 g 把正四面体的顶点变成顶点. 我们用 $g \circ i$ 表示 g 把顶点 i 变成的顶点. 显然，对于任意 $g_1, g_2 \in G$，有 $(g_1 g_2) \circ i = g_1 \circ (g_2 \circ i)$；$I \circ i = i$，很自然地我们称群 G 在顶点集合 Ω 上有一个作用. 由此受到启发，抽象出下述重要概念：

定义 1 设 G 是一个群，Ω 是一个非空集合. 如果 $G \times \Omega$ 到 Ω 有一个映射：$(a, x) \mapsto a \circ x$，满足

$$(ab) \circ x = a \circ (b \circ x), \forall a, b \in G, \forall x \in \Omega; \tag{1}$$

$$e \circ x = x, \forall x \in \Omega. \tag{2}$$

则称群 G 在集合 Ω 上有一个**作用**(action).

等式(1) 表明，两个元素乘积的作用等于相继作用；等式(2) 表

明，单位元的作用等于恒等作用（即保持 Ω 的每一个元素不动）.

上面给群 G 在集合 Ω 上的作用下的定义是朴素的，直观的．下面我们深入地分析一下群 G 在集合 Ω 上的作用到底是什么意思．从定义 1 看到，任意给定 $a \in G$，引起了 Ω 的一个变换：$x \mapsto a \circ x$．我们把这个变换记作 $\psi(a)$，下面的命题 1 指出了 ψ 是什么.

命题 1　设群 G 在集合 Ω 上有一个作用．任意给定 $a \in G$，令

$$\psi(a)x \xlongequal{\text{def}} a \circ x, \quad \forall\, x \in \Omega, \tag{3}$$

则 ψ 是群 G 到 Ω 的全变换群 S_Ω 的一个同态.

证明　从(3)式看到，$\psi(a)$ 是 Ω 的一个变换．对于任意 $a, b \in G$，我们有

$$\begin{aligned}\psi(ab)x &= (ab) \circ x = a \circ (b \circ x) \\ &= \psi(a)[\psi(b)x] = [\psi(a)\psi(b)]x, \ \forall\, x \in \Omega.\end{aligned}$$

因此　$\psi(ab) = \psi(a)\psi(b), \ \forall\, a, b \in G.$　(4)

从而对于任意 $a \in G$，有

$$\begin{aligned}[\psi(a)\psi(a^{-1})]x &= \psi(aa^{-1})x = \psi(e)x \\ &= e \circ x = x, \quad \forall\, x \in \Omega.\end{aligned}$$

因此　$$\psi(a)\psi(a^{-1}) = 1_\Omega. \tag{5}$$

同理，　$$\psi(a^{-1})\psi(a) = 1_\Omega. \tag{6}$$

(5)、(6)式表明 $\psi(a)$ 是 Ω 的可逆变换，从而 $\psi(a) \in S_\Omega$．因此 ψ 是 G 到 S_Ω 的一个映射．(4)式表明 ψ 保持运算，因此 ψ 是群 G 到 S_Ω 的一个同态.　□

请读者验证，命题 1 的逆命题也成立，即，如果群 G 到非空集合 Ω 的全变换群 S_Ω 有一个同态 ψ，令

$$a \circ x \xlongequal{\text{def}} \psi(a)x, \quad \forall\, a \in G, \quad \forall\, x \in \Omega, \tag{7}$$

则群 G 在集合 Ω 上有一个作用：$(a, x) \mapsto a \circ x$.

设群 G 在集合 Ω 上有一个作用，据命题 1，它引起了群 G 到 S_Ω 的一个同态 ψ．我们把同态 ψ 的核 $\mathrm{Ker}\psi$ 称为这个**作用的核**．显然群

G 中元素a 属于作用的核当且仅当$a \circ x = x, \forall x \in \Omega$. 如果作用的核仅由单位元 e 组成,则称这个作用是**忠实的**(faithful),此时 ψ 是群 G 到 S_Ω 的单同态.

群在集合上的作用是一把双刃剑. 对于群来说,可以通过群在适当集合上的各种作用来研究群的结构. 对于集合 Ω 来说,可以选择合适的群在 Ω 上的作用来研究 Ω 的性质,特别是有关 Ω 的计数. 我们先来看前者,讨论群在适当集合上的若干重要作用,并且利用这些作用来研究群的结构.

1. 群 G 在集合 G 上的左平移

设 G 是一个群,令

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, x) &\longmapsto ax. \end{aligned} \tag{8}$$

显然有$(ab)x = a(bx), ex = x, \forall x \in G, \forall a, b \in G$. 因此(8)式给出了群 G 在集合G 上的一个作用,称这个作用为群 G 在集合G 上的**左平移**(left translation).

G 中元素a 属于左平移的核当且仅当$ax = x, \forall x \in G$,由此推出,$a = e$. 因此左平移是忠实的. 从而它引起了群 G 到 S_G 的一个单同态 ψ. 于是 $G \cong \mathrm{Im}\psi$. 由于 $\mathrm{Im}\psi < S_G$,因此群 G 与集合 G 的一个变换群同构. 这样我们证明了下述定理:

定理 2(Cayley 定理) 任意一个群都同构于某一集合上的变换群. □

由定理 2 立即得到

推论 3 任意一个有限群都同构于一个置换群. □

历史上最早研究的群是置换群(伽罗瓦在 1830 年前后研究的群)和变换群(克莱因在 1872 年提出爱尔朗根纲领). 随着研究的深入,人们逐渐认识到这些群中元素本身的内容并不重要,重要的是关联这些元素的运算及其所服从的规则. 于是开始研究抽象群. 这方面早期的探索者有凯莱(Cayley),F.G. Frobenius 等. Cayley定理及其推

论的意义在于指出了任何一个抽象群本质上是变换群(对于无限群而言)或置换群(对于有限群而言).

类似地可以讨论群 G 在集合 G 上的右平移.

2. 群 G 在左商集 $(G/H)_l$ 上的左平移

设 G 是一个群,$H < G$.令

$$G \times (G/H)_l \longrightarrow (G/H)_l$$
$$(a, xH) \longmapsto axH. \tag{9}$$

显然,对于任意 $a, b \in G$,有

$(ab) \circ xH = (ab)xH = a(bx)H = a \circ b \circ xH, \quad \forall xH \in (G/H)_l.$

$$e \circ xH = exH = xH, \quad \forall xH \in (G/H)_l.$$

因此(9)式给出了群 G 在左商集 $(G/H)_l$ 上的一个作用,称它为群 G 在 $(G/H)_l$ 上的**左平移**.

类似地可以讨论群 G 在右商集 $(G/H)_r$ 上的右平移.

3. 群 G 在集合 G 上的共轭作用

令
$$G \times G \longrightarrow G$$
$$(a, x) \longmapsto axa^{-1}. \tag{10}$$

对于任意 $a, b \in G$,任意 $x \in G$,有

$$(ab) \circ x = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1}$$
$$= a(b \circ x)a^{-1} = a \circ (b \circ x),$$
$$e \circ x = exe^{-1} = x.$$

因此(10)式给出了群 G 在集合 G 上的一个作用,称它为群 G 在集合 G 上的**共轭作用**(conjugation action).

群 G 在集合 G 上的共轭作用的核是什么?

$$a \text{ 属于共轭作用的核} \Longleftrightarrow a \circ x = x, \forall x \in G$$
$$\Longleftrightarrow axa^{-1} = x, \forall x \in G$$
$$\Longleftrightarrow ax = xa, \forall x \in G. \tag{11}$$

令　　$Z(G) \xlongequal{\text{def}} \{a \in G \mid ax = xa, \quad \forall x \in G\}$.　　(12)

称 $Z(G)$ 是群 G 的**中心**(centre). 上述推导过程表明，群 G 在集合 G 上的共轭作用的核等于 $Z(G)$.

群 G 在集合 G 上的共轭作用引起了群 G 到 S_G 的一个同态 σ. 上面已求出了同态核 $\mathrm{Ker}\sigma = Z(G)$. 下面来讨论同态象 $\mathrm{Im}\sigma$ 是什么. 我们把 G 中元素 a 在同态 σ 下的像 $\sigma(a)$ 记成 σ_a. 于是

$$\sigma_a(x) = axa^{-1}, \quad \forall x \in G. \tag{13}$$

由于 $\sigma_a \in S_G$，因此 σ_a 是 G 到 G 的一个双射. 对于任意 $x, y \in G$，有

$$\sigma_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \sigma_a(x)\sigma_a(y), \tag{14}$$

因此 σ_a 是群 G 到 G 的一个同构映射.

群 G 到自身的一个同构映射称为 G 的一个**自同构**(automorphism). 由(13)式定义的 σ_a 称为 G 的由 a 决定的**内自同构**(inner automorphism).

容易看出，群 G 的所有自同构组成的集合对于映射的乘法成一个群，称它为 G 的**自同构群**(automorphism group)，记作 $Aut(G)$.

群 G 的所有内自同构组成的集合正好是上面所说的群 G 到 S_G 的同态 σ 的像 $\mathrm{Im}\sigma$. 我们知道 $\mathrm{Im}\sigma$ 是 S_G 的子群，称它是 G 的**内自同构群**，记作 $Inn(G)$. 显然 $Inn(G) < Aut(G)$.

对于任意给定的 $\tau \in Aut(G)$，任取 $\sigma_a \in Inn(G)$，有

$$\begin{aligned}(\tau\sigma_a\tau^{-1})x &= \tau\sigma_a(\tau^{-1}x) = \tau[a(\tau^{-1}x)a^{-1}] \\ &= \tau(a)[\tau(\tau^{-1}x)]\tau(a^{-1}) = \tau(a)x\tau(a)^{-1} \\ &= \sigma_{\tau(a)}(x), \quad \forall x \in G.\end{aligned}$$

因此 $\tau\sigma_a\tau^{-1} = \sigma_{\tau(a)} \in Inn(G)$. 从而 $Inn(G)$ 是 $Aut(G)$ 的正规子群.

从上面的讨论知道，群 G 到 S_G 的同态 σ 的核等于 $Z(G)$，σ 的象等于 $Inn(G)$，于是据群同态基本定理，得

$$G/Z(G) \cong Inn(G). \tag{15}$$

这样我们利用群 G 在集合 G 上的共轭作用，得到了下述结论：

定理 4 群 G 的内自同构群 $Inn(G)$ 同构于群 G 对于中心 $Z(G)$ 的商群 $G/Z(G)$. □

为了利用群 G 在集合 Ω 上的作用来研究群 G 的结构，以及了解集合 Ω 的性质，我们需要引进下面一些概念，并且推导有关结论.

定义 2 设群 G 在集合 Ω 上有一个作用，对于 $x \in \Omega$，令

$$G(x) \xlongequal{\text{def}} \{g \circ x \mid g \in G\}, \tag{16}$$

称 $G(x)$ 是 x 的**轨道**(orbit).

如果群 G 在集合 Ω 上有一个作用，则所有轨道组成的集合给出了 Ω 的一个划分. 理由如下：

在集合 Ω 中规定一个二元关系如下：

$$x \sim y \overset{\text{def}}{\Longleftrightarrow} \text{存在 } g \in G, \text{使得 } y = g \circ x. \tag{17}$$

容易验证 ~ 是等价关系. 由 x 确定的等价类 $\bar{x}$ 为

$$\begin{aligned} \bar{x} &= \{y \in \Omega \mid x \sim y\} \\ &= \{y \in \Omega \mid \text{存在 } g \in G, \text{使得 } y = g \circ x\} \\ &= \{g \circ x \mid g \in G\} \\ &= G(x). \end{aligned} \tag{18}$$

因此所有轨道(即等价类)组成的集合给出了 Ω 的一个划分. 由于轨道就是等价类，因此任意两条轨道或者相等，或者不相交. 于是有

$$\Omega = \bigcup_{i \in I} G(x_i), \tag{19}$$

其中 $G(x_i) \cap G(x_j) = \varnothing$，当 $i \neq j$. 我们把集合 $\{x_i \mid i \in I\}$ 称为 Ω 的 G - 轨道的完全代表系.

如果群 G 在集合 Ω 上的作用只有一条轨道，即对于任意 $x, y \in \Omega$，存在 $g \in G$ 使得 $y = g \circ x$，则称 G 在 Ω 上的这个作用是**传递的**(transitive). 此时称 Ω 是群 G 的一个**齐性空间**(homogeneous space).

例如，群 G 在左商集 $(G/H)_l$ 上的左平移是传递的，这是因为对于任意 xH、$yH \in (G/H)_l$，有

$$(yx^{-1}) \circ xH = yx^{-1}xH = yH,$$

从而左商集$(G/H)_l$就是群G的一个齐性空间.

考虑群G在集合G上的共轭作用，x的轨道为

$$G(x) = \{gxg^{-1} \mid g \in G\}. \tag{20}$$

我们把(20)式右端的集合称为x的**共轭类**(conjugacy class).从(20)式看出，x的共轭类就是群G在集合G上的共轭作用下x的轨道.从而群G的任意两个共轭类或者相等，或者不相交.从共轭类的定义看出，x的共轭类只含一个元素当且仅当$x \in Z(G)$.于是当G是有限群时，从(19)式可得出

$$|G| = |Z(G)| + \sum_{j=1}^{r} |G(x_j)|, \tag{21}$$

其中$G(x_j)$是x_j的共轭类，$\{x_1, \cdots, x_r\}$是G里非中心元素的共轭类的完全代表系.我们把(21)式称为有限群G的**类方程**(class equation).给定$x \in G$，任取$g \in G$，gxg^{-1}称为x的**共轭元素**(conjugacy elements).

定义3　设群G在集合Ω上有一个作用.给定$x \in \Omega$，令

$$G_x \xlongequal{\text{def}} \{g \in G \mid g \circ x = x\}, \tag{22}$$

称G_x是x的**稳定子**(stabilizer).

容易验证，G_x是G的一个子群.因此也称G_x是x的**稳定子群**.

考虑群G在集合G上的共轭作用，x的稳定子是什么?

$$\begin{aligned} G_x &= \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\}. \end{aligned} \tag{23}$$

我们把(23)式右端的集合称为x在G里的**中心化子**(centralizer)，记作$C_G(x)$，它就是在群G的共轭作用下x的稳定子群.

在x的轨道与x的稳定子之间有密切联系:

定理5(轨道—稳定子定理)　设群G在集合Ω上有一个作用，则对于任意给定的$x \in \Omega$，有

$$|G(x)| = [G:G_x],\tag{24}$$

即，x 的轨道的基数等于 x 的稳定子在 G 中的指数.

证明 令 $\varphi: G(x) \longrightarrow (G/G_x)_l$

$$a \circ x \longmapsto aG_x.$$

由于

$$\begin{aligned} a \circ x = b \circ x &\Longleftrightarrow b^{-1} \circ (a \circ x) = b^{-1} \circ (b \circ x) \\ &\Longleftrightarrow (b^{-1}a) \circ x = (b^{-1}b) \circ x \\ &\Longleftrightarrow (b^{-1}a) \circ x = x \\ &\Longleftrightarrow b^{-1}a \in G_x \\ &\Longleftrightarrow aG_x = bG_x. \end{aligned}$$

因此 φ 是 $G(x)$ 到 $(G/G_x)_l$ 的一个映射，并且 φ 是单射. 显然 φ 是满射，从而 φ 是双射. 因此 $G(x)$ 与 $(G/G_x)_l$ 有相同的基数，即 $|G(x)| = [G:G_x]$. □

推论 6 如果有限群 G 在集合 Ω 上有一个作用，则每一条轨道的长(即轨道的基数)是 G 的阶的因子，即

$$|G| = |G_x||G(x)|.\tag{25}$$

证明 $|G| = |G_x|[G:G_x] = |G_x||G(x)|$. □

考虑有限群 G 在集合 G 上的共轭作用，据轨道一稳定子定理，得

$$|G(x)| = [G:C_G(x)],\tag{26}$$

即，x 的共轭类所含元素的个数等于 x 的中心化子在 G 中的指数.

下面我们来介绍群在集合上作用的一些应用.

设群 G 在集合 Ω 上有一个作用，令

$$\Omega_0 \xlongequal{\text{def}} \{x \in \Omega \mid g \circ x = x,\ \forall g \in G\},\tag{27}$$

称 Ω_0 是群 G **的不动点集**.

设 G 是有限群，如果 G 的阶是素数 p 的方幂，即 $|G| = p^m$，$m \geqslant 1$，则称 G 是 $p-$**群**.

命题 7 设 $p-$ 群 G 在有限集合 Ω 上有一个作用，则

$$|\Omega_0| \equiv |\Omega| \pmod{p}. \tag{28}$$

证明 从(19)式得出

$$|\Omega| = \sum |G(x_i)| = |\Omega_0| + \sum_{j=1}^{r} |G(x_j)|, \tag{29}$$

其中$|G(x_j)| > 1, j = 1,2,\cdots,r$. 据推论6得,$|G(x_j)|$是$|G|$的因子,而$|G| = p^m, m \geqslant 1$,因此$|G(x_j)| = p^{s_j}, 0 < s_j \leqslant m, j = 1, 2, \cdots, r$. 于是由(29)式得

$$|\Omega| \equiv |\Omega_0| \pmod{p}.$$ □

推论 8 p-群必有非平凡的中心(即不等于$\{e\}$).

证明 设G是p-群. 考虑群G在集合G上的共轭作用,则群G的不动点集$\Omega_0 = Z(G)$. 据命题7得

$$|Z(G)| \equiv |G| \equiv 0 \pmod{p}.$$

又由于$Z(G)$是G的子群,因此$|Z(G)| = p^s$,对某个$s > 0$. 从而$Z(G) \neq \{e\}$. □

利用推论8,我们可以决定p^2阶群的互不同构的类型,其中p是素数.

例 1 设p是素数,则p^2阶群或者是循环群,或者同构于$\mathbf{Z}_p \times \mathbf{Z}_p$. 从而$p^2$阶群都是abel群.

证明 设群G的阶是p^2. 如果G含有p^2阶元,则G是循环群. 否则,G的每个非单位元都是p阶元. 据推论8,$Z(G) \neq \{e\}$. 于是可在$Z(G)$中取一个非单位元a. 由于$|\langle a\rangle| = p$,因此在G中可取一个非单位元$b \overline{\in} \langle a\rangle$. 由于$|\langle b\rangle| = p$,因此$\langle a\rangle \cap \langle b\rangle = \{e\}$. 据习题1.2的第14题,得

$$|\langle a\rangle\langle b\rangle| = \frac{|\langle a\rangle||\langle b\rangle|}{|\langle a\rangle \cap \langle b\rangle|} = p^2.$$

因此$G = \langle a\rangle\langle b\rangle$,由于$a \in Z(G)$,因此$\langle a\rangle$的每个元素与$\langle b\rangle$的每个元素可交换,于是据§3的定理4得,

$$G \cong \langle a\rangle \times \langle b\rangle.$$

由于$\langle a\rangle$,$\langle b\rangle$都同构于$\mathbf{Z}_p$,因此$G\cong \mathbf{Z}_p\times\mathbf{Z}_p$. □

命题 9 设群G在集合Ω上有一个作用,则同一条轨道上的点,它们的稳定子群彼此共轭,从而这些稳定子群的基数相同.

证明 设x,y属于同一条轨道,则存在$a\in G$,使得$y=a\circ x$,任取$h\in G_x$,则

$$\begin{aligned}(aha^{-1})\circ y &= (aha^{-1})\circ(a\circ x)=ah\circ[(a^{-1}a)\circ x]\\ &=(ah)\circ x=a\circ(h\circ x)=a\circ x=y.\end{aligned}$$

因此$aha^{-1}\in G_y$,从而$aG_xa^{-1}\subseteq G_y$.

由于$x=a^{-1}\circ y$,因此同理可证,$a^{-1}G_ya\subseteq G_x$,从而$G_y\subseteq aG_xa^{-1}$.由此得出,$G_y=aG_xa^{-1}$,即G_y与G_x共轭.容易看出,$h\mapsto aha^{-1}$是G_x到G_y的一个双射,因此$|G_x|=|G_y|$. □

利用命题 9,我们可以求出有限群作用在有限集合上的轨道条数.

定理 10(Burnside 引理) 设有限群G在有限集合Ω上有一个作用,用$F(g)$表示g的不动点集,即

$$F(g)\xlongequal{\text{def}}\{x\in\Omega\mid g\circ x=x\}. \tag{30}$$

则轨道条数r为

$$r=\frac{1}{|G|}\sum_{g\in G}|F(g)|. \tag{31}$$

即,轨道条数等于平均被G的一个元素保持不动的点的数目.

证明 考虑$G\times\Omega$的下述子集:

$$S=\{(g,x)\mid g\circ x=x\}. \tag{32}$$

给定$g\in G$,令

$$\begin{aligned}S(g,\cdot)&\xlongequal{\text{def}}\{x\in\Omega\mid(g,x)\in S\}\\ &=\{x\in\Omega\mid g\circ x=x\}=F(g).\end{aligned}$$

给定$x\in\Omega$,令

$$S(\cdot,x)\xlongequal{\text{def}}\{g\in G\mid(g,x)\in S\}$$

$$= \{g \in G \mid g \circ x = x\} = G_x.$$

由于 $\sum_{g \in G} |S(g, \cdot)| = |S| = \sum_{x \in \Omega} |S(\cdot, x)|$，因此

$$\sum_{g \in G} |F(g)| = \sum_{x \in \Omega} |G_x|. \tag{33}$$

设 $\{x_1, x_2, \cdots, x_r\}$ 是 Ω 的 G-轨道的完全代表系，则 $\Omega = \bigcup_{i=1}^{r} G(x_i)$，其中 $G(x_i) \cap G(x_j) = \emptyset$，当 $i \neq j$. 据命题 9，在轨道 $G(x_i)$ 里的每一个点，它的稳定子群与 G_{x_i} 有相同的阶. 因此我们有

$$\sum_{x \in \Omega} |G_x| = \sum_{i=1}^{r} \sum_{x \in G(x_i)} |G_x| = \sum_{i=1}^{r} |G(x_i)| |G_{x_i}|$$

$$= \sum_{i=1}^{r} |G| = r|G|. \tag{34}$$

从(33)、(34)式立即得出公式(31). □

从物质的分子结构等实际问题抽象出一个数学模型：对一个正多面体的顶点用若干种颜色染色，问有多少种不同的染色方案？下面看一个例子.

例 2 正四面体的 4 个顶点用 4 种颜色染色，求真正不同的染色方案的个数.

解 由于每一个顶点有 4 种颜色可供染色，因此总共有 4^4 个染色方案，它们组成的集合记作 Ω，如果两个染色方案能够通过正四面体的旋转对称(性)群 G 中某一个旋转从一个方案变成另一个方案，则很自然地认为这两个染色方案本质上是一样的. 因此 Ω 在群 G 作用下的同一条轨道上的染色方案本质上是相同的. 从而真正不同的染色方案的个数等于轨道条数.

一个染色方案可以用一个 4 元组表示：

$$\{1_{i_1}, 2_{i_2}, 3_{i_3}, 4_{i_4}\}, \tag{35}$$

其中 1_{i_1} 表示顶点 1 染第 i_1 种颜色，其余类推.

群 G 首先作用在顶点集 $W = \{1, 2, 3, 4\}$ 上. G 的每一个元素 g

诱导了 W 的一个置换,记作 $\bar{g}$,称 $\bar{g}$ 是 g 的置换表示,例如,绕顶点 1 与对面中心的连线转角为 $\frac{2\pi}{3}$ 的旋转 σ_1 的置换表示是 $\bar{\sigma}_1 = (1)(234)$. 参看本节开头的图 1-6. 对于 $g \in G$,令

$$g \circ \{1_{i_1}, 2_{i_2}, 3_{i_3}, 4_{i_4}\} \xlongequal{\text{def}} \{\bar{g}(1)_{i_1}, \bar{g}(2)_{i_2}, \bar{g}(3)_{i_3}, \bar{g}(4)_{i_4}\}.$$

容易验证上式给出了群 G 在集合 Ω 上的一个作用,为了求轨道条数 r,先求 g 的不动点数 $|F(g)|$. 以 σ_1 为例. 显然,一个染色方案在 σ_1 下保持不动当且仅当顶点 2,3,4 染同一种颜色,即 $\bar{\sigma}_1$ 的轮换表示中同一个轮换里的顶点染同一种颜色. $\bar{\sigma}_1$ 有两个轮换,每个轮换有 4 种颜色可供染色,于是 σ_1 保持不动的染色方案有 4^2 个. 即 $|F(\sigma_1)| = 4^2$. 容易看出,G 的每一个非单位元 g 的置换表示 $\bar{g}$ 都有两个轮换,因此 $|F(g)| = 4^2, \forall g \neq I$. 而 $|F(I)| = 4^4$. 于是

$$r = \frac{1}{12}(4^4 + 11 \times 4^2) = 36.$$

因此真正不同的染色方案有 36 个.

例 2 的解法适用于一般情形. 类似地可证下述结论:

定理 11(Pólya 定理) 设有限群 G 作用在 n 个对象组成的集合 W 上. G 中元素 g 在 W 上的置换表示记作 $\bar{g}$. 用 m 种颜色给 W 里的 n 个对象染色,则真正不同的染色方案的个数 r 为

$$r = \frac{1}{|G|}\sum_{g \in G} m^{r(\bar{g})}, \tag{36}$$

其中 $r(\bar{g})$ 是 $\bar{g}$ 的轮换表示中轮换的个数(包括 1-轮换).

习题 1.5

1. 令
$$\begin{aligned} \mathbf{Z} \times \mathbf{R} &\longrightarrow \mathbf{R} \\ (n, x) &\longmapsto n + x, \end{aligned}$$

说明这个映射给出了整数加群 $\mathbf{Z}$ 在实数集 $\mathbf{R}$ 上的一个作用.

2. 令
$$\mathbf{Z}\times\mathbf{R}\longrightarrow\mathbf{R}$$
$$(n,x)\longmapsto(-1)^n x,$$
说明这个映射给出了整数加群 **Z** 在实数集 **R** 上的一个作用.

3. 证明:映射 $\sigma: x\mapsto x^{-1}$ 是任一 abel 群 G 的一个自同构.

4. 设 F 是一个域,求 $GL_n(F)$ 的中心.

*5. $GL_2(\mathbf{C})$ 的每一个元素
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
引起了扩充复平面 $\mathbf{C}\cup\{\infty\}$ 上的一个变换:
$$z\longmapsto\frac{az+b}{cz+d},$$
称它为 **Möbius 变换**. 证明:

(1) 所有 Möbius 变换组成的集合 G 对于变换的乘法成一个群,称它为 **Möbius 群**;

(2)
$$GL_2(\mathbf{C})/Z(GL_2(\mathbf{C}))\cong G.$$

6. 设 G 是一个群,证明:如果 $G/Z(G)$ 是循环群,则 G 是 abel 群.

7. 分别求 D_{2m-1}, D_{2m} 的中心,其中 $m\geqslant 2$.

*8. 求 S_n 的中心,其中 $n\geqslant 3$.

9. 分别求 U_6, U_9 的自同构群.

*10. 求 $\mathbf{Z}_2\times\mathbf{Z}_2$ 的自同构群.

*11. 求 S_3 的自同构群.

*12. 群 G 的一个子群 H 称为 G 的**特征子群**(characteristic subgroup)如果 G 的每一个自同构把 H 映成 H 自身,即对于所有的 $\tau\in Aut(G)$,有 $\tau(H)=H$. 证明 G 的中心 $Z(G)$ 和 G 的换位子群 G' 都是 G 的特征子群.

13. 分别求 D_5, D_6 的所有共轭类.

*14. 分别求 D_{2m-1}, D_{2m} 的所有共轭类，其中 $m \geqslant 2$.

15. S_n 中，设 σ 的不相交的轮换分解式(包含所有的 1－轮换）为

$$\sigma = (a_1 a_2 \cdots a_{l_1})(b_1 b_2 \cdots b_{l_2}) \cdots (q_1 q_2 \cdots q_{l_t}),$$

其中 $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_t$，且 $l_1 + l_1 + \cdots + l_t = n$. 则我们把有序数组 $(l_1, l_2, \cdots, l_t)$ 称为置换 σ 的**型**(type)，也称为 n 的一个**分拆**(partition). 证明：

(1) σ_1 与 σ_2 在 S_n 中共轭当且仅当 σ_1 与 σ_2 同型；

(2) S_n 中共轭类的个数等于 n 的分拆的个数.

*16. 求 S_4 的共轭类的个数，以及每个共轭类的代表和元素数目.

*17. 求 A_4 的共轭类的个数，以及每个共轭类的代表和元素数目.

*18. S_n 中，σ 是一个 n － 轮换. 求 σ 的共轭类的元素数目，以及 $C_{S_n}(\sigma)$.

*19. 求 O_2 的所有共轭类.

*20. 证明：群 G 的子群 H 为正规子群当且仅当 H 是 G 的一些共轭类的并集.

*21. (1) 求 S_5 的共轭类的个数，以及每个共轭类的代表和元素数目.

(2) 证明：S_5 只有三个正规子群，即 $\{(1)\}, A_5, S_5$.

*22. 设 G 为 p － 群，$N \triangleleft G$，且 $|N| = p$. 证明：$N \subseteq Z(G)$.

23. 设 G 是一个群，G 的所有子群组成的集合记作 Ω. 令 $G \times \Omega \to \Omega; (a, H) \mapsto aHa^{-1}$. 容易看出这给出了群 G 在 Ω 上的一个作用. H 的轨道 $G(H)$ 是由 H 的所有共轭子群组成的. H 的稳定子群 $G_H = \{g \in G \mid gHg^{-1} = H\}$ 称为 H 在 G 中的**正规化子**(normalizer)，记作 $N_G(H)$. 显然，$H \triangleleft N_G(H)$. 证明：如果 G 为有限群，$H < G$，则 H 的共轭子群的个数等于 $[G : N_G(H)]$.

*24. 设 H 是有限群 G 的一个非平凡子群，证明：

$$G \neq \bigcup_{g \in G} gHg^{-1}$$

*25. 设 G 为一个 $2k$ 阶群，k 为奇数．证明：G 必有指数为 2 的子群．

*26. 设 G 为一个有限群，$H < G$，且 $|G:H| = n > 1$．证明：G 或者有一个指数整除 $n!$ 的非平凡正规子群，或者 G 同构于 S_n 的一个子群．

*27. 设 G 为一个有限群，p 为 $|G|$ 的最小素因子．证明：指数为 p 的子群（如果存在）必为正规子群．

*28. 正方体的 6 个面用红、绿两种颜色染色，求真正不同的染色方案的个数．

*29. 设群 G 在集合 Ω 和 Ω' 上分别有一个作用"$\circ$"和"$\cdot$"．如果在 Ω 与 Ω' 之间有一个双射 ψ，使得

$$\psi(a \circ x) = a \cdot (\psi(x)), \quad \forall a \in G, \quad x \in \Omega.$$

也就是，使得下面的图 1－7 可交换：

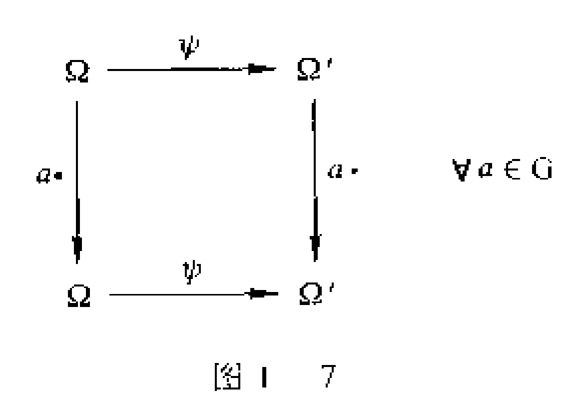


图 1－7

则称 G 的这两个作用是**等价的**(equivalent)．

证明　群 G 在任一集合 Ω 上的传递作用等价于群 G 在左商集 $(G/G_x)_l$ 上的左平移，其中 $x \in \Omega$．

*30. 设 N 和 H 是两个群，并且 H 到 $Aut(N)$ 有一个同态 ψ．在集合 $N \times H$ 上定义一个二元运算如下：

$$(n_1,h_1)(n_2,h_2) \xlongequal{\text{def}} (n_1\cdot\varphi(h_1)(n_2), h_1\cdot h_2),$$

证明 $N\times H$ 成为一个群，称它为 N 与 H 的**半直积**(semidirect product)，记作 $N\rtimes H$.

令 $\tilde{N}=\{(n,e)\mid n\in N\}$，证明：$\tilde{N}\lhd N\rtimes H$，$\tilde{N}\cong N$.

*31. 设群 G 与群 H 分别作用在集合 Ω 和 W 上.令

$$(g,h)\circ(x,y) \xlongequal{\text{def}} (g\circ x, h\circ y),$$

证明这给出了群 $G\times H$ 在集合 $\Omega\times W$ 上的一个作用，称它是乘积作用(product action).求 $\Omega\times W$ 里的元素 (x,y) 的轨道 $(G\times H)(x,y)$，以及 (x,y) 的稳定子群 $(G\times H)_{(x,y)}$.

§6 Sylow 定理

本章 §2 的 Lagrange 定理指出，有限群 G 的任一子群的阶是 $|G|$ 的因子.反之，对于 $|G|$ 的任一正因子 d，是否存在一个 d 阶子群？我们已经看到，这对于有限循环群是成立的.但是对于交错群 A_4，它的阶是 12，却没有 6 阶子群(参看习题 1.2 的第 11 题).而 A_4 有 2 阶，3 阶，4 阶子群.6 是两个素数 2 与 3 的乘积；2，3，4 都是一个素数的方幂.自然会问：当 $|G|$ 的正因子 d 是一个素数的方幂时，是否存在 d 阶子群？本节介绍的 Sylow 定理将回答这一问题.我们需要一个引理：

引理 设 $n=p^l m$，$(m,p)=1$，p 是素数，则对于任意 $k\leqslant l$，有

$$p^{l-k}\mid C_n^{p^k},\quad p^{l-k+1}\nmid C_n^{p^k}. \tag{1}$$

证明

$$C_n^{p^k}=\frac{n(n-1)\cdots(n-j)\cdots(n-p^k+1)}{p^k(p^k-1)\cdots(p^k-j)\cdots 1}.$$

我们来证 $(n-j)$ 与 (p^k-j) 含有的 p 的方幂相同，当 $1\leqslant j\leqslant$

$p^k - 1$. 设 $j = p^t j'$，其中 $(j', p) = 1$，$0 \leqslant t < k$，则

$$n - j = p^l m - p^t j' = p^t(p^{l-t}m - j'),$$
$$p^k - j = p^k - p^t j' = p^t(p^{k-t} - j').$$

由于 $l \geqslant k > t$，且 $(m, p) = 1$，$(j', p) = 1$，因此 $(p^{l-t}m - j')$ 与 $(p^{k-t} - j')$ 均不含因子 p，从而 $n - j$ 与 $p^k - j$ 含有的 p 的方幂是一样的，都为 p^t. 于是有

$$r = \frac{(n-1)\cdots(n-p^k+1)}{(p^k-1)\cdots 1} = \frac{b}{a},$$

其中 $(a, p) = 1$，$(b, p) = 1$，从而

$$C_n^{p^k} = \frac{n}{p^k} \cdot \frac{b}{a} = p^{l-k}\frac{mb}{a}.$$

由于 $C_n^{p^k}$ 是整数，因此 $a \mid p^{l-k}mb$. 由于 $(a, p) = 1$，因此 $a \mid mb$. 从而 p^{l-k} 是 $C_n^{p^k}$ 的一个因子，而 $\frac{mb}{a}$ 不含因子 p. 由此得出(1)式. □

定理 1(Sylow 第一定理) 设群 G 的阶为 $n = p^l m$，其中 p 为素数，$(m, p) = 1$，$l > 0$，则对于 $1 \leqslant k \leqslant l$，$G$ 中必有 p^k 阶子群. 其中 p^l 阶子群(即 p 的最高方幂阶子群)称为 G 的 **Sylow p - 子群.**

想法(idea) 如果群 G 在某个集合 Ω 上有一个作用，则 Ω 的某个元素 x 的稳定子群 G_x 就是 G 的一个子群. 关键是选择适当的集合 Ω.

证明 设 Ω 是 G 的所有 p^k 元子集组成的集合，Ω 的一个元素形如

$$A = \{a_1, a_2, \cdots, a_{p^k}\},$$

于是 $|\Omega| = C_n^{p^k}$. 对于 $g \in G$，令

$$g \circ A \xlongequal{\text{def}} \{ga_1, ga_2, \cdots, ga_{p^k}\}, \tag{2}$$

容易看出这给出了群 G 在 Ω 上的一个作用. 于是

$$\Omega = \bigcup_{i} G(A_i), \quad G(A_i) \cap G(A_j) = \emptyset, \text{当 } i \neq j. \tag{3}$$

从而
$$|\Omega| = \sum_{j=1}^{r} |G(A_j)|. \tag{4}$$
由引理 1 知，
$$p^{l-k+1} \nmid |\Omega|.$$
因此至少有一条轨道 $G(A_j)$ 满足 $p^{l-k+1} \nmid |G(A_j)|$. 根据轨道—稳定子定理的推论，有
$$|G| = |G(A_j)||G_{A_j}|. \tag{5}$$
由于 p^l 恰好整除 $|G|$，且 $|G(A_j)|$ 含有的 p 因子至多为 p^{l-k}，因此 $|G_{A_j}|$ 含有的 p 因子至少为 p^k. 即
$$|G_{A_j}| = p^k q \geqslant p^k. \tag{6}$$

另一方面，对于任意 $g \in G_{A_j}$，有 $g \circ A_j = A_j$. 于是对于 $a \in A_j$，有 $ga \in A_j$，从而
$$G_{A_j}a = \{ga \mid g \in G_{A_j}\} \subseteq A_j,$$
于是
$$|G_{A_j}a| \leqslant |A_j| = p^k.$$
又由于右陪集 $G_{A_j}a$ 与子群 G_{A_j} 有相同的阶，因此
$$|G_{A_j}| \leqslant p^k. \tag{7}$$
从(6)、(7) 式得，$|G_{A_j}| = p^k$. 即 G_{A_j} 就是 G 的一个 p^k 阶子群. □

由于对于 $g \in G$，有 $h \mapsto ghg^{-1}$ 是子群 H 到它的共轭子群 gHg^{-1} 的双射，因此 H 与 gHg^{-1} 有相同的阶. 从而如果 P 是 G 的 Sylow p－子群，则 P 的任一共轭子群也是 G 的 Sylow p－子群. 反之，G 的任意两个 Sylow p－子群是否共轭?

定理 2(Sylow 第二定理)　设群 G 的阶为 $n = p^l m$，其中 p 为素数，$(m,p) = 1$，$l > 0$，则

(1) 对于 $1 \leqslant k \leqslant l$，$G$ 的任意一个 p^k 阶子群一定包含在 G 的某一个 Sylow p－子群中；

(2) G 的任意两个 Sylow p－子群在 G 中共轭.

证明 (1) 设 H 是 G 的任意一个 p^k 阶子群，$1 \leqslant k \leqslant l$. 任取 G 的一个 Sylow p - 子群 P. 考虑 p - 群 H 在 G 对 P 的左陪集 $(G/P)_l$ 上的左平移，即

$$h \circ (gP) \xlongequal{\text{def}} (hg)P. \tag{8}$$

用 Ω_0 表示 H 的不动点集，则

$$|\Omega_0| \equiv |(G/P)_l| = m \not\equiv 0 \pmod p. \tag{9}$$

从而存在 $aP \in \Omega_0$，即 $\forall h \in H$，有 $h \circ (aP) = aP$，也就是 $(ha)P = aP$，从而 $a^{-1}ha \in P$. 由此得出，$\forall h \in H$，有 $h \in aPa^{-1}$，因此

$$H \subseteq aPa^{-1},$$

即 H 包含在 G 的一个 Sylow p - 子群 aPa^{-1} 中.

(2) 设 P_1、P_2 是 G 的任意两个 Sylow p - 子群. 由刚才证得的结论（把 P_1 看成上述的 H，把 P_2 看成上述的 P）得，存在 $a \in G$，使得 $P_1 \subseteq aP_2a^{-1}$. 由于 $|P_1| = |aP_2a^{-1}|$，因此 $P_1 = aP_2a^{-1}$. □

推论 3 有限群 G 的 Sylow p - 子群是正规子群当且仅当 G 的 Sylow p - 子群的个数为 1.

证明 G 的子群 P 是正规子群当且仅当 P 的所有共轭子群都等于 P 自身. 再结合 Sylow 第二定理即得结论. □

从推论 3 看出，我们要会求 G 的 Sylow p - 子群的个数.

定理 4（Sylow 第三定理） 设群 G 的阶 $n = p^l m$，其中 p 是素数，$(m, p) = 1$，$l > 0$. 则 G 的 Sylow p - 子群的个数 r 模 p 同余于 1，并且 r 是 m 的因子. 即

$$r \equiv 1 \pmod p, \text{且 } r \mid m. \tag{10}$$

想法(idea) 要证 $r \equiv 1 \pmod p$，促使我们考虑 p - 群在 r 元集合 Ω 上的作用，并且去求不动点集 Ω_0.

证明 用 Ω 表示 G 的所有 Sylow p - 子群组成的集合，即 $\Omega = \{P_1, P_2, \cdots, P_r\}$. 于是，$|\Omega| = r$. 考虑 P_1 在 Ω 上的共轭作用，即对于任意 $a \in P_1$，令

$$a \circ P_i \xrightarrow{\text{def}} aP_ia^{-1}. \tag{11}$$

容易验证这的确是一个作用. 我们来求 P_1 的不动点集 Ω_0. 对于 $Q \in \Omega$,我们有

$$\begin{aligned} Q \in \Omega_0 &\Longleftrightarrow a \circ Q = Q, \forall a \in P_1 \\ &\Longleftrightarrow aQa^{-1} = Q, \forall a \in P_1 \\ &\Longleftrightarrow a \in N_G(Q), \forall a \in P_1 \\ &\Longleftrightarrow P_1 \subseteq N_G(Q), \end{aligned}$$

其中 $N_G(Q)$ 是 Q 在 G 中的正规化子,它的定义是

$$N_G(Q) \xlongequal{\text{def}} \{g \in G \mid gQg^{-1} = Q\}.$$

由定义看出,$Q \lhd N_G(Q)$. 由于 P_1, Q 是 G 的 Sylow p - 子群,当然它们也是 $N_G(Q)$ 的 Sylow p - 子群. 由于 $Q \lhd N_G(Q)$,因此据推论 3 得,$Q = P_1$. 因此 $\Omega_0 = \{P_1\}$. 从而

$$r = |\Omega| \equiv |\Omega_0| \equiv 1 \pmod p.$$

从习题 1.5 的第 23 题知道,P_1 的共轭子群的个数等于 $[G : N_G(P_1)]$. 即 $r = [G : N_G(P_1)]$. 从而 $r \mid |G|$,即 $r \mid p^l m$. 由于 $r \equiv 1 \pmod p$,因此 $(r, p) = 1$. 从而 $r \mid m$. □

Sylow 定理在研究有限群的结构中起着十分重要的作用. 让我们来看几个例子.

例 1　证明不存在阶为 **12** 的单群.

证明　设群 G 的阶为 12. 由于 $12 = 2^2 \times 3$,因此 G 有 Sylow 2 - 子群. 设 G 的 Sylow 2 - 子群的个数为 r. 由 Sylow 第三定理得,$r = 1 + 2k$,且 $r \mid 3$. 由此推出,$k = 0$ 或 1. 即 $r = 1$ 或 3.

情形 1　如果 $r = 1$,则 G 的 Sylow 2 - 子群 P 是 G 的正规子群.

情形 2　如果 $r = 3$,则 G 的 Sylow 2 - 子群有三个:P_1, P_2, P_3,它们组成集合 Ω. 群 G 在 Ω 上有共轭作用. 由此作用引起群 G 到 S_3

的一个同态 ψ. 从而

$$G/\mathrm{Ker}\psi \cong \mathrm{Im}\psi.$$

由于 $\mathrm{Im}\psi < S_3$, 因此 $|\mathrm{Im}\psi| \leqslant 6$. 而 $|G| = 12$. 因此 $\mathrm{Ker}\psi \neq \{e\}$. 假如 $\mathrm{Ker}\psi = G$, 则对于所有的 $g \in G$, 都有 $gP_1g^{-1} = P_1$. 于是 $P_1 \lhd G$, 这与 $r = 3$ 矛盾. 因此 $\mathrm{Ker}\psi$ 是 G 的非平凡正规子群.

综上述得, 12 阶群 G 不是单群. □

例 2 设 p 是奇素数, 决定 $2p$ 阶群的类型(即, 互不同构的类型. 今后不再每次声明).

解 设 G 是 $2p$ 阶群. 据 Sylow 第一定理, G 有 p 阶子群 P 和 2 阶子群 H. 由于素数阶群一定是循环群, 因此 $P = \langle a \rangle$, $H = \langle b \rangle$. 由于 $[G:P] = 2$, 因此 $P \lhd G$. 由于 $b \notin \langle a \rangle$, 因此 G 对于 $\langle a \rangle$ 的右陪集分解式是 $G = \langle a \rangle \cup \langle a \rangle b$. 从而 G 的 $2p$ 个元素为

$$e, a, \cdots, a^{p-1}, b, ab, \cdots, a^{p-1}b.$$

据 Lagrange 定理, ab 的阶只可能是 $2p, p, 2$. 如果 $|ab| = 2p$, 则 $G = \langle ab \rangle$, 它同构于 $\mathbf{Z}_{2p}$. 如果 ab 的阶为 2, 则 $abab = e$, 从而 $bab = a^{-1}$. 此时

$$G = \langle a, b \mid a^p = b^2 = e,\ bab = a^{-1} \rangle.$$

容易看出, $G \cong D_p$. 假如 $|ab| = p$, 则 $(ab)^p = e$. 由于 $\langle a \rangle \lhd G$, 因此有

$$\begin{aligned}\langle a \rangle &= \langle a \rangle (ab)^p = (\langle a \rangle ab)^p = (\langle a \rangle b)^p \\ &= \langle a \rangle b^p = \langle a \rangle b,\end{aligned}$$

矛盾. 从而 $|ab| \neq p$.

综上述得, 如果 p 为素数, 则 $2p$ 阶只有两种类型: 或者同构于 $\mathbf{Z}_{2p}$, 或者同构于 D_p.

我们已经知道, $\mathbf{Z}_8, \mathbf{Z}_4 \times \mathbf{Z}_2, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, D_4$ 都是 8 阶群. 还有没有其它的 8 阶群?

在 18 世纪末和 19 世纪初, C. Wessel(1797), R. Argand(1806),

高斯(Gauss,1831) 分别给出了复数 $a+bi$ 的几何表示,这样复数才有了合法的地位,从那以后,数学家们认识到复数能用来表示和研究平面上的向量,进而应用到物理上.但是数学家不久就发现,复数的应用是受到限制的.例如,当几个力作用于一个物体时,这些力不一定在一个平面上.因此需要把复数加以推广.首先想到3维向量.但是向量的内积不是代数运算.向量的外积虽然是代数运算,但是它既不满足交换律,又不满足结合律,与复数乘法相去甚远.对复数的推广作出重要贡献的是哈密顿(W.R.Hamilton),他经过长期努力,于1843年发现他所要找的新数应包含四个分量,而且必须放弃乘法的交换性.他把这种新数命名为**四元数**(quaternion).

哈密顿的四元数形如

$$a+bi+cj+dk, \tag{12}$$

其中 a,b,c,d 为实数,$\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 满足

$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{k}^2=-1, \tag{13}$$

$$\boldsymbol{ij}=-\boldsymbol{ji}=\boldsymbol{k},\ \boldsymbol{jk}=-\boldsymbol{kj}=\boldsymbol{i},\ \boldsymbol{ki}=-\boldsymbol{ik}=\boldsymbol{j}. \tag{14}$$

两个四元数相乘可以根据上面的规则仿照复数乘法那样去做.哈密顿证明了四元数乘法具有"结合性".四元数是历史上第一次构造的不满足乘法交换律的数系.哈密顿本人曾对于四元数的发现,作过一个生动的描述:

"明天是四元数的第15个生日.1843年10月16日,当我和哈密顿太太步行去都柏林途中来到勃洛翰桥的时候,它们就来到了人世间,或者说出生了,发育成熟了.这就是说,此时此地我感到思想的电路接通了,而从中落下的火花就是 $\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 之间的基本方程,恰恰就是我后来使用它们的那个样子.我当场抽出笔记本(它还保存着),将这些思想记录下来.……"

据说,他当时还取出随身带的一把小刀,将四元数所满足的规律刻在了那座桥的石栏上.(注:哈密顿的上述一段话,引自《数学史教程》,李文林著,高等教育出版社和施普林格出版社2000年出版,第

215 页).

所有四元数组成的集合用 $\boldsymbol{H}$ 表示. 它对于四元数的加法(类似于复数的加法)和乘法成为一个有单位元的非交换环,并且每个非零元都可逆. 它比域只少一个乘法交换律. 我们称 $\boldsymbol{H}$ 是**四元数体**(quaternion field).

考虑四元数体 $\boldsymbol{H}$ 的一个子集:

$$Q=\{\pm 1,\pm \boldsymbol{i},\pm \boldsymbol{j},\pm \boldsymbol{k}\}. \tag{15}$$

从(13)、(14)式看出,Q 对于四元数的乘法封闭,并且每个元素的逆仍在 Q 中. 因此 Q 成为一个群. 称它是**四元数群**(quaternion group). 从(13)、(14)式得到

$$\boldsymbol{i}^4=1,\quad \boldsymbol{j}^4=1,\quad \boldsymbol{i}^{-1}=-\boldsymbol{i},\quad \boldsymbol{j}^{-1}=-\boldsymbol{j},$$
$$\boldsymbol{jij}^{-1}=(-\boldsymbol{k})(-\boldsymbol{j})=\boldsymbol{kj}=-\boldsymbol{i}=\boldsymbol{i}^{-1}.$$

因此

$$Q=\langle \boldsymbol{i},\boldsymbol{j}\mid \boldsymbol{i}^4=\boldsymbol{j}^4=1,\boldsymbol{jij}^{-1}=\boldsymbol{i}^{-1}\rangle. \tag{16}$$

由于 Q 是非交换群,因此 Q 不同构于 $\mathbf{Z}_8,\mathbf{Z}_4\times\mathbf{Z}_2,\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$. 由于 Q 的二阶元只有 -1,因此 Q 不同构于 D_4(D_4 有 4 个二阶元). 8 阶群除了这五种类型外,还有别的类型吗?

*例 3 决定 8 阶群的类型.

解 设 G 是 8 阶群. 如果 G 有一个 8 阶元,则 G 是循环群,它同构于 $\mathbf{Z}_8$. 下面设 G 没有 8 阶元. 据 Sylow 第一定理,G 必有 4 阶子群 H. 由于 $[G:H]=2$,因此 $H\lhd G$. 4 阶群只有两种:循环群,或者 Klein 群.

情形 1 G 有 4 阶循环子群 H. 设 $H=\langle a\rangle$. 则 G 对于 $\langle a\rangle$ 的右陪集分解式为 $G=\langle a\rangle\cup\langle a\rangle b$. 从而 G 的 8 个元素为

$$e,a,a^2,a^3,b,ab,a^2b,a^3b.$$

据 Lagrange 定理,b 的阶为 4 或 2. 因为 $b\notin\langle a\rangle$,所以 $b^2\notin\langle a\rangle b$. 从而 $b^2\in\langle a\rangle$. 由于 $|b^2|=\dfrac{|b|}{(|b|,2)}$,因此当 $|b|=4$ 时,$|b^2|=2$,

从而 $b^2=a^2$；当 $|b|=2$ 时，$b^2=e$. 此外我们考察 ba. 显然 $ba\overline{\in}\langle a\rangle$，且 ba 不等于 b（否则，$a=e$，矛盾）. 假如 $ba=a^2b$，则 $a=b^{-1}a^2b$，从而 $a^2=(b^{-1}a^2b)(b^{-1}a^2b)=e$，矛盾. 因此 $ba=ab$ 或 $ba=a^3b$. 根据 b^2 和 ba 的可能性，我们分下述四种情形讨论.

(i) $ba=ab, b^2=e$. 此时 G 是 abel 群，考虑 G 到 $\mathbf{Z}_4\times\mathbf{Z}_2$ 的一个映射 $\sigma: a\mapsto(\overline{1},\overline{0}), b\mapsto(\overline{0},\overline{1})$. 容易验证 σ 是一个同构映射. 从而 $G\cong\mathbf{Z}_4\times\mathbf{Z}_2$.

(ii) $ba=ab, b^2=a^2$. 此时 G 是 abel 群. 由于 $(ab^{-1})^2=a^2b^{-2}=a^2a^{-2}=e$，因此 ab^{-1} 是2阶元. 令 $a\mapsto(\overline{1},\overline{0}), ab^{-1}\mapsto(\overline{0},\overline{1})$. 容易验证这给出了 G 到 $\mathbf{Z}_4\times\mathbf{Z}_2$ 的一个同构映射. 从而 $G\cong\mathbf{Z}_4\times\mathbf{Z}_2$.

(iii) $ba=a^3b, b^2=e$. 此时 $bab=a^{-1}$. 因此

$$G=\langle a,b\,|\,a^4=b^2=e,\ bab=a^{-1}\rangle.$$

从而 $G\cong D_4$.

(iv) $ba=a^3b, b^2=a^2$. 此时 $bab^{-1}=a^{-1}$. 因此

$$G=\langle a,b\,|\,a^4=b^4=e,\ bab^{-1}=a^{-1}\rangle.$$

与(16)式比较，令 $a\mapsto\boldsymbol{i}$, $b\mapsto\boldsymbol{j}$，容易验证这给出了 G 到四元数群 $\boldsymbol{Q}$ 的一个同构映射. 从而 $G\cong\boldsymbol{Q}$.

情形2 G 没有4阶循环子群，从而 G 的4阶子群 $H\cong\mathbf{Z}_2\times\mathbf{Z}_2$. 设 $H=\{e,a,b,ab\}$，其中 a,b,ab 都是2阶元. 设 G 对于 H 的右陪集分解式为 $G=H\cup Hc$. 从而 G 的8个元素为

$$e,a,b,ab,c,ac,bc,abc.$$

令 $K=\langle c\rangle$. 容易看出 $G=HK$，且 $H\cap K=\{e\}$. 由于 G 的每个非单位元都是2阶元，因此 G 必为 abel 群(参看习题1.2的第8题). 据 §3 的定理4得，$G\cong H\times K$. 由于 $K\cong\mathbf{Z}_2$，因此 $G\cong\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$.

综上述得，12阶群 G 只有五种互不同构的类型. 它们的代表分别是：

$$\mathbf{Z}_8, \mathbf{Z}_4 \times \mathbf{Z}_2, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2, D_4, Q.$$

习题 1.6

1. 证明不存在阶为 148 的单群.

2. 证明不存在阶为 36 的单群.

3. 证明不存在阶为 56 的单群.

*4. 证明不存在阶为 30 的单群.

5. 证明 6 阶群或者是循环群,或者同构于 S_3.

*6. 决定 10 阶群的类型.

7. 决定 15 阶群的类型.

*8. 决定 35 阶群的类型.

*9. 决定 21 阶群的类型.

*10. 设 p、q 都是素数,且 $p < q$. 证明:

(1) 如果 $q \not\equiv 1 \pmod p$,则 pq 阶群是循环群;

(2) 如果 $q \not\equiv 1 \pmod p$,则 pq 阶群是具有正规 Sylow p - 子群的非交换群,或者是循环群;

*11. 设 p,q 是不同的素数. 证明 p^2q 阶群必包含一个正规的 Sylow 子群.

*12. 设群 G 的阶为 p^3,其中 p 是素数. 证明:如果 G 是非交换群,则 $|Z(G)| = p$,且 $Z(G) \quad G'$.

*13. 设 p 是素数. 计算 S_p 中 Sylow p - 子群的个数. 由此证明 Wilson 定理:$(p-1)! \equiv -1 \pmod p$.

*14. 设 G 为一个有限群,$N \lhd G$,P 是 N 的一个 Sylow p - 子群. 证明:$G = N \cdot N_G(P)$.

*15. 证明:如果有限群 G 有一个循环的 Sylow 2 - 子群,则 G 有一个指数为 2 的子群.

§7 有限 abel 群的结构

这一节我们来研究有限 abel 群的结构,我们先看几个具体的例子.

4 阶群都是 abel 群,它们有两种互不同构的类型,代表分别是 $\mathbf{Z}_4,\mathbf{Z}_2\times\mathbf{Z}_2$.

6 阶群有两种互不同构的类型,代表分别是 $\mathbf{Z}_6,D_3$,其中 D_3 是非 abel 群;$\mathbf{Z}_6$ 是 abel 群,且 $\mathbf{Z}_6\cong\mathbf{Z}_2\times\mathbf{Z}_3$.

9 阶群都是 abel 群,它们有两种互不同构的类型,代表分别是 $\mathbf{Z}_9,\mathbf{Z}_3\times\mathbf{Z}_3$.

8 阶 abel 群有三种互不同构的类型,它们的代表分别是 $\mathbf{Z}_8,\mathbf{Z}_2\times\mathbf{Z}_4,\mathbf{Z}_2\times\mathbf{Z}_2\times\mathbf{Z}_2$.

由此看出,这些 abel 群都同构于循环群或者循环群的直积,并且每个循环群的阶都是一个素数的方幂,这些循环群的阶组成的有重集合,例如对于 8 阶 abel 群,有三种情形:

$$\{2^3\},\quad \{2,2^2\},\quad \{2,2,2\}.$$

它们分别对应于 8 写成素数方幂乘积的所有三种可能:

$$8=2^3,\quad 8=2\times 2^2,\quad 8=2\times 2\times 2.$$

任意有限 abel 群是否也有这样的结构?

设 G 是有限 abel 群,它的阶为

$$n=p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s},$$

其中 $p_1,p_2,\cdots,p_s$ 是两两不同的素数,$l_i>0$,$i=1,2,\cdots,s$.

据 Sylow 第一定理,G 有 Sylow p_i-子群 H_i,$i=1,2,\cdots,s$. 由于 $p_i\neq p_j$,因此 $H_i\cap H_j=\{e\}$. 从而

$$|H_iH_j|=\frac{|H_i||H_j|}{|H_i\cap H_j|}=p_i^{l_i}p_j^{l_j}.$$

用数学归纳法容易证明

$$|H_1H_2\cdots H_s| = p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}.$$

因此
$$G = H_1H_2\cdots H_s.$$

又由于 G 是 abel 群，因此从 §3 的定理 4 容易得出

$$G \cong H_1 \times H_2 \times \cdots \times H_s, \tag{1}$$

即，G 同构于它的 Sylow p_i－子群（$i = 1,2,\cdots,s$）的直积.

下一步自然要去研究 abel p－群的结构. 从 8 阶 abel 群的结构受到启发，我们猜想有下述结论：

定理 1 设 P 是 abel p－群，$|P| = p^l$. 则

$$P \cong \mathbf{Z}_{p^{k_1}} \times \mathbf{Z}_{p^{k_2}} \times \cdots \times \mathbf{Z}_{p^{k_r}}, \tag{2}$$

其中 $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_r$，且 $k_1 + k_2 + \cdots + k_r = l$. 称有重集合

$$\{p^{k_1}, p^{k_2}, \cdots, p^{k_r}\}$$

是 P 的**初等因子**（elementary divisors）.

想法（idea） 先证 $P \cong \langle a_1\rangle \times P_1$，其中 $\langle a_1\rangle, P_1$ 都是 P 的子群，然后用数学归纳法. 为此需要证：

$$P = \langle a_1\rangle P_1，且 \langle a_1\rangle \cap P_1 = \{e\}.$$

从 $P = \langle a_1\rangle P_1$ 知道，a_1 属于 P 的一个生成元集. 但是一个群的生成元集不唯一，并且不同生成元集的元素个数可能不相等. 例如，

$$S_n = \langle (12),(13),\cdots,(1n)\rangle,$$

$$S_n = \langle (12),(123\cdots n)\rangle.$$

显然 S_n 不能由一个元素生成. 因此称 $\{(12),(123\cdots n)\}$ 是 S_n 的一个极小生成元集. 一般地，设群 G 有一个生成元集 W 含 r 个元素，而 G 的任何 $r-1$ 个元素都不能生成 G，则称 W 是 G 的一个**极小生成元集**（minimal set of generators）. 对于有限群（或有限生成的群）G，一定存在极小生成元集（因为自然数集 $\mathbf{N}$ 的任一非空子集里必有最小数）. G 的极小生成元集不唯一. 从定义可看出，G 的任何两个极小生成元集含有的元素个数相同. 这样我们就可以在定理 1 的证明

中，对 abel p－群的极小生成元集含有的元素个数作数学归纳法，并且应当从 P 的一个极小生成元集中去找上述的元素 a_1.

还需要 $\langle a_1\rangle \cap P_1 = \{e\}$. 假如 $\langle a_1\rangle \cap P_1 \neq \{e\}$，则存在 $0 < c < |a_1|$，使得 $a_1^c \in P_1$. 设 $P_1 = \langle b_2, \cdots, b_r\rangle$，则

$$a_1^c = b_2^{l_2}\cdots b_r^{l_r},$$

即
$$a_1^c b_r^{-l_r}\cdots b_2^{-l_2} = e. \tag{3}$$

我们把(3)式称为 P 的**生成元 $a_1, b_2, \cdots, b_r$ 的一个关系**. 设 $|a_1| = m_1$，则 $a_1^{m_1} = e$，从而有生成元的另一个关系：

$$a_1^{m_1} b_r^0 \cdots b_2^0 = e. \tag{4}$$

为了能得出矛盾，注意到 $c < m_1$. 我们应当在 P 的所有极小生成元集的全部关系中，从生成元的正的幂指数组成的集合里选取一个最小的正整数，设为 m_1，然后找 a_1 使得 a_1 的阶为 m_1. 于是从(3)、(4)两式可得出矛盾，从而保证 $\langle a_1\rangle \cap P_1 = \{e\}$.

证明 对 abel p－群的极小生成元集所含元素的个数 n 作数学归纳法. 当 $n = 1$ 时，这是循环群，于是命题为真. 设 $n = r - 1$ 时，命题为真. 现在来看 $n = r$ 的情形，在 abel p－群 P 的所有极小生成元集的全部关系中，从生成元的正的幂指数组成的集合里选取一个最小的正整数，设为 m_1. 不妨设 P 的一个极小生成元集 $\{x_1, x_2, \cdots, x_r\}$ 中有一个关系为

$$x_1^{m_1} x_2^{j_2} \cdots x_r^{j_r} = e. \tag{5}$$

我们断言 $m_1 \mid j_2$. 理由如下：设 $j_2 = qm_1 + u, 0 \leqslant u < m_1$，则

$$e = x_1^{m_1} x_2^{qm_1+u} x_3^{j_3}\cdots x_r^{j_r} = (x_1 x_2^q)^{m_1} x_2^u x_3^{j_3}\cdots x_r^{j_r}.$$

容易看出，$\{x_1x_2^q, x_2, x_3, \cdots, x_r\}$ 也是 P 的一个极小生成元集. 于是从 m_1 的选择知道，必有 $u = 0$. 从而 $j_2 = qm_1$. 同理可证，$m_1 \mid j_v$，于是 $j_v = q_v m_1, 3 \leqslant v \leqslant r$. 因此(5)式成为

$$x_1^{m_1} x_2^{qm_1} x_3^{q_3 m_1} \cdots x_r^{q_r m_1} = e,$$

即
$$(x_1 x_2^{q_2} x_3^{q_3}\cdots x_r^{q_r})^{m_1} = e, \tag{6}$$
令
$$a_1 = x_1 x_2^{q_2} x_3^{q_3}\cdots x_r^{q_r}, \tag{7}$$
则
$$x_1 = a_1 x_r^{-q_r}\cdots x_3^{-q_3} x_2^{-q_2}.$$
从而$\{a_1, x_2, x_3, \cdots, x_r\}$也是 P 的一个极小生成元集．从(6)式得，$a_1^{m_1} = e$，从 m_1 的选择知道，m_1 是 a_1 的阶．因此 $m_1 = p^{k_1}$，其中 k_1 是某个正整数．令
$$P_1 = \langle x_2, x_3, \cdots, x_r\rangle. \tag{8}$$
于是
$$P = \langle a_1, P_1\rangle. \tag{9}$$
假如$\langle a_1\rangle \cap P_1 \neq \{e\}$，则存在 $1 \leqslant s_1 \leqslant m_1$，使得 $a_1^{s_1} \in P_1$．从而有 $a_1^{s_1} = x_2^{s_2}\cdots x_r^{s_r}$．由此得出
$$a_1^{s_1} x_r^{-s_r}\cdots x_2^{-s_2} = e \tag{10}$$
这与 m_1 的选择矛盾，因此$\langle a_1\rangle \cap P_1 = \{e\}$．又由于 P 是 abel 群，因此
$$P \cong \langle a_1\rangle \times P_1 \tag{11}$$
$\{x_2, x_3, \cdots, x_r\}$必为 P_1 的一个极小生成元集．对 P_1 重复上述做法．在 P_1 的所有极小生成元集的全部关系中，从生成元的正的幂指数组成的集合里选取一个最小的正整数，设为 m_2．不妨设 P_1 的一个极小生成元集$\{y_2, y_3, \cdots, y_r\}$有一个关系为
$$y_2^{m_2} y_3^{n_3}\cdots y_r^{n_r} = e. \tag{12}$$
同理可证 $m_2 = p^{k_2}$，其中 k_2 是某个正整数．从(12)式得
$$a_1^{m_1} y_2^{m_2} y_3^{n_3}\cdots y_r^{n_r} = e. \tag{13}$$
由于容易看出$\{a_1, y_2, y_3, \cdots, y_r\}$也是 P 的一个极小生成元集，因此从(13)式可得出，$m_1 | m_2$(与前面证 $m_1 | n_2$ 的方法一样)．于是 $k_1 \leqslant k_2$.

对 P_1 用数学归纳法，并且注意上面的论述可得

$$P_1 \cong \mathbf{Z}_{p^{k_2}} \times \mathbf{Z}_{p^{k_3}} \times \cdots \times \mathbf{Z}_{p^{k_r}}, \tag{14}$$

其中 $k_2 \leqslant k_3 \leqslant \cdots \leqslant k_r, k_2 + k_3 + \cdots + k_r = l - k_1$.

由于 $\langle a_1 \rangle \cong \mathbf{Z}_{p^{k_1}}$，因此从(11)、(14)式得

$$P \cong \mathbf{Z}_{p^{k_1}} \times \mathbf{Z}_{p^{k_2}} \times \mathbf{Z}_{p^{k_3}} \times \cdots \times \mathbf{Z}_{p^{k_r}},$$

其中 $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_r$，且 $k_1 + k_2 + \cdots + k_r = l$. □

结合(1)式和定理1便得到

定理 2 设 G 是 n 阶 abel 群，$n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$，其中 $p_1, p_2, \cdots, p_s$ 是两两不同的素数，$l_i > 0, i = 1, 2, \cdots, s$，则

$$G \cong \mathbf{Z}_{p_1^{k_{11}}} \times \mathbf{Z}_{p_1^{k_{12}}} \times \cdots \times \mathbf{Z}_{p_1^{k_{1r_1}}} \times \cdots \times \mathbf{Z}_{p_s^{k_{s1}}} \times \cdots \times \mathbf{Z}_{p_s^{k_{sr_s}}}, \tag{15}$$

其中 $k_{i1} \leqslant k_{i2} \leqslant \cdots \leqslant k_{ir_i}$，且 $k_{i1} + k_{i2} + \cdots + k_{ir_i} = l_i, i = 1, 2, \cdots, s$. 称有重集合 $\{p_1^{k_{11}}, \cdots, p_1^{k_{1r_1}}, \cdots, p_s^{k_{s1}}, \cdots, p_s^{k_{sr_s}}\}$ 是 G 的**初等因子**. □

容易看出，如果两个有限 abel 群有相同的初等因子，那么它们同构. 反之如何？我们来探讨这个问题.

设 G_1 和 G_2 都是有限 abel 群，并且设 $G_1 \cong G_2$，则它们的阶相同. 设它们的阶为 $n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$，则 G_i 同构于它的 Sylow 子群的直积($i = 1, 2$)：

$$G_1 \cong H_1 \times H_2 \times \cdots \times H_s, \tag{16}$$

$$G_2 \cong K_1 \times K_2 \times \cdots \times K_s, \tag{17}$$

其中 H_j, K_j 分别是 G_1, G_2 的 Sylow p_j - 子群，$1 \leqslant j \leqslant s$. 由同构关系的对称性和传递性得

$$H_1 \times H_2 \times \cdots \times H_s \cong K_1 \times K_2 \times \cdots \times K_s. \tag{18}$$

设同构映射为 ψ. 由于

$$(h_1, h_2, \cdots, h_s)^{p_1^{l_1}} = (h_1^{p_1^{l_1}}, h_2^{p_1^{l_1}}, \cdots, h_s^{p_1^{l_1}}),$$

因此从$(h_1,h_2,\cdots,h_s)^{p_1^i}=(e,e,\cdots,e)$可推出$h_2=\cdots=h_s=e$. 于是$H_1\times H_2\times\cdots\times H_s$里的$p_1^i$阶元必形如$(h_1,e,e,\cdots,e)$. 同理$K_1\times K_2\times\cdots\times K_s$里的$p_1^i$阶元必形如$(k_1,e,e,\cdots,e)$. 由于同构映射$\psi$把$p_1^i$阶元映成$p_1^i$阶元, 因此$\psi(h_1,e,e,\cdots,e)=(k_1,e,e,\cdots,e)$, 其中$h_1$是$H_1$里的任一$p_1^i$阶元, k_1是K_1里某一个确定的p_1^i阶元(它依赖于h_1). 于是ψ诱导了H_1到K_1的一个映射ψ_1, 即$\psi_1(h_1)$等于上式中的k_1. 由于ψ是单射, 因此ψ_1也是单射. 由于ψ是满射, 因此ψ_1也是满射. 由于ψ保持运算, 因此ψ_1也保持运算. 从而ψ_1是H_1到K_1的一个同构映射, 于是$H_1\cong K_1$. 同理可证$H_j\cong K_j$, $j=2,\cdots,s$. 这就证明了: 如果两个有限 abel 群同构, 则它们的 Sylow p - 子群同构(对于群的阶的每一个素因子p).

现在设H和K都是 abel p - 群, 它们同构, 则它们的阶相同. 设它们的阶为p^l, $l>0$. 据定理 1, 有

$$H\cong \mathbf{Z}_{p^{k_1}}\times\mathbf{Z}_{p^{k_2}}\times\cdots\times\mathbf{Z}_{p^{k_r}},\tag{19}$$

$$K\cong \mathbf{Z}_{p^{l_1}}\times\mathbf{Z}_{p^{l_2}}\times\cdots\times\mathbf{Z}_{p^{l_t}},\tag{20}$$

其中

$$k_1\leqslant k_2\leqslant\cdots\leqslant k_r,\quad k_1+k_2+\cdots+k_r=l,$$
$$l_1\leqslant l_2\leqslant\cdots\leqslant l_t,\quad l_1+l_2+\cdots+l_t=l.$$

用$\widetilde{H},\widetilde{K}$分别表示(19),(20)式中右端的直积, 于是有$\widetilde{H}\cong\widetilde{K}$. 首先我们想证明$r=t$.

设$\widetilde{H}_1$是$\widetilde{H}$中所有p阶元组成的集合, 容易验证$\widetilde{H}_1$是$\widetilde{H}$的子群. 我们想定义有限域$\mathbf{Z}_p$与$\widetilde{H}_1$的纯量乘法. 对于$\bar{i}\in\mathbf{Z}_p$, $\alpha\in\widetilde{H}_1$, 令

$$\bar{i}\alpha\stackrel{\text{def}}{=\!=}i\alpha.\tag{21}$$

如果$\bar{i}=\bar{j}$, 则$p\mid(i-j)$. 从而$(i-j)\alpha=0$, 即$i\alpha=j\alpha$. 因此(21)式的确定义了$\mathbf{Z}_p$与$\widetilde{H}_1$的纯量乘法. 容易验证$\widetilde{H}_1$对于加法和纯量乘

法成为域 $\mathbf{Z}_p$ 上的一个线性空间.令

$$\varepsilon_i = (\bar{0},\cdots,\bar{0},\underset{\text{第 } i \text{ 位}}{\bar{1}},\bar{0},\cdots,\bar{0}),$$

$i = 1,2,\cdots,r$,在 $\widetilde{H}_1$ 中任取一个元素 α,则

$$\alpha = (\bar{a}_1,\bar{a}_2,\cdots,\bar{a}_r) = a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_r\varepsilon_r. \tag{22}$$

由于

$$\begin{aligned} 0 = p\alpha &= pa_1\varepsilon_1 + pa_2\varepsilon_2 + \cdots + pa_r\varepsilon_r \\ &= (\overline{pa_1},\overline{pa_2},\cdots,\overline{pa_r}), \end{aligned} \tag{23}$$

因此 $p^{k_i} \mid pa_i$,从而 $a_i = p^{k_i-1}b_i$,对某个 $b_i \in \mathbf{Z}$.于是

$$\alpha = b_1 p^{k_1-1}\varepsilon_1 + b_2 p^{k_2-1}\varepsilon_2 + \cdots + b_r p^{k_r-1}\varepsilon_r. \tag{24}$$

显然 $p^{k_i-1}\varepsilon_i$ 是 $\widetilde{H}$ 的 p 阶元,因此它属于 $\widetilde{H}_1$,$1 \leqslant i \leqslant r$.容易验证,$p^{k_1-1}\varepsilon_1, p^{k_2-1}\varepsilon_2,\cdots,p^{k_r-1}\varepsilon_r$ 线性无关.因此它是域 $\mathbf{Z}_p$ 上线性空间 $\widetilde{H}_1$ 的一个基,从而 $\dim\widetilde{H}_1 = r$.

同理可证,$\widetilde{K}$ 中所有 p 阶元组成的集合 $\widetilde{K}_1$ 是域 $\mathbf{Z}_p$ 上线性空间,并且 $\dim\widetilde{K}_1 = t$.

设 f 是 $\widetilde{H}$ 到 $\widetilde{K}$ 的同构映射.由于同构映射把 p 阶元映成 p 阶元,因此 f 诱导了群 $\widetilde{H}_1$ 到 $\widetilde{K}_1$ 的同构映射 f_1.容易看出,f_1 保持纯量乘法.因此 f_1 是域 $\mathbf{Z}_p$ 上线性空间 $\widetilde{H}_1$ 到 $\widetilde{K}_1$ 的同构映射.从而 $\dim\widetilde{H}_1 = \dim\widetilde{K}_1$.即 $r = t$.

其次我们想证明 $k_i = l_i$,$i = 1,2,\cdots,r$.用反证法.假如 $k_1 = l_1,\cdots,k_{u-1} = l_{u-1}$,$k_u \neq l_u$,其中 $1 \leqslant u \leqslant r$.不妨设 $k_u < l_u$.令

$$\widetilde{H}_2 \xlongequal{\text{def}} \{p^{k_u}\beta \mid \beta \in \widetilde{H}\}, \quad \widetilde{K}_2 \xlongequal{\text{def}} \{p^{k_u}\gamma \mid \gamma \in \widetilde{K}\}.$$

显然 $\widetilde{H}_2 < \widetilde{H}$,$\widetilde{K}_2 < \widetilde{K}$.容易看出

$$\widetilde{H}_2 = 0 \times \cdots \times 0 \times p^{k_u}\mathbf{Z}_{p^{k_{u+1}}} \times \cdots \times p^{k_u}\mathbf{Z}_{p^{k_r}}, \tag{25}$$

$$\widetilde{K}_2 = 0 \times \cdots \times 0 \times p^{k_u}\mathbf{Z}_{p^{l_u}} \times \cdots \times p^{k_u}\mathbf{Z}_{p^{l_r}}, \tag{26}$$

其中

$$p^{k_u}\mathbf{Z}_{p^t} \xlongequal{\text{def}} \{p^{k_u}\bar{\delta} \mid \bar{\delta} \in \mathbf{Z}_{p^t}\}. \tag{27}$$

容易看出，$p^{k_u}\mathbf{Z}_{p^t}$ 是 $\mathbf{Z}_{p^t}$ 的子群，从而它也是循环群，因此它同构于 $\mathbf{Z}_{p^{c_1}}$，其中 $c_1 \leqslant t$. 于是从(25)，(26) 式得出，$\widetilde{H}_2$ 是至多 $r-u$ 个 p 的方幂阶循环群的直积，$\widetilde{K}_2$ 是 $r-u+1$ 个 p 的方幂阶循环群的直积. 群 $\widetilde{H}$ 到 $\widetilde{K}$ 的同构映射 f 诱导了 $\widetilde{H}_2$ 到 $\widetilde{K}_2$ 的一个映射 f_2：$f_2(p^{k_u}\beta) \xlongequal{\text{def}} p^{k_u}f(\beta)$. 容易看出，$f_2$ 是群 $\widetilde{H}_2$ 到 $\widetilde{K}_2$ 的同构映射. 因此 $\widetilde{H}_2 \cong \widetilde{K}_2$. 运用上面对 $\widetilde{H}$，$\widetilde{K}$ 证得的结果(从 $\widetilde{H} \cong \widetilde{K}$ 得出 $r = t$)得，$\widetilde{H}_2$ 的直积表达式中循环群的个数 q 与 $\widetilde{K}_2$ 的直积表达式中循环群的个数 $r-u+1$ 相等，但是 $q \leqslant r-u < r-u+1$，矛盾. 因此 $k_i = l_i$，$1 \leqslant i \leqslant r$.

综上述得下面的定理 3：

定理 3 两个有限 abel 群同构当且仅当它们的初等因子相同. □

定理 3 表明，初等因子是有限 abel 群组成的集合在同构关系下的完全不变量.

定理 2 和定理 3 把有限 abel 群的结构完全搞清楚了.

例 1 决定 200 阶 abel 群的互不同构的类型.

解 $200 = 2^3 \times 5^2$. 由于 3 的分拆有：$3 = 3$，$3 = 2 + 1$，$3 = 1 + 1 + 1$；2 的分拆有：$2 = 2$，$2 = 1 + 1$，因此 200 阶 abel 群的初等因子有下述 6 种可能情形：

$$\{2^3, 5^2\}, \ \{2^3, 5, 5\}, \ \{2, 2^2, 5^2\},$$
$$\{2, 2^2, 5, 5\}, \ \{2, 2, 2, 5^2\}, \ \{2, 2, 2, 5, 5\},$$

从而 200 阶 abel 群有 6 种互不同构的类型，它们的代表分别是

$$\mathbf{Z}_{2^3} \times \mathbf{Z}_{5^2}, \quad \mathbf{Z}_{2^3} \times \mathbf{Z}_5 \times \mathbf{Z}_5, \quad \mathbf{Z}_2 \times \mathbf{Z}_{2^2} \times \mathbf{Z}_{5^2},$$
$$\mathbf{Z}_2 \times \mathbf{Z}_{2^2} \times \mathbf{Z}_5 \times \mathbf{Z}_5, \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{5^2},$$
$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5 \times \mathbf{Z}_5.$$

其中 $\mathbf{Z}_{2^3}\times\mathbf{Z}_{5^2}\cong\mathbf{Z}_{200}$，这是循环群.

例 2　设 $G\cong\mathbf{Z}_5\times\mathbf{Z}_{15}\times\mathbf{Z}_{36}$，求 G 的初等因子.

解　$$\begin{aligned}G&\cong\mathbf{Z}_5\times\mathbf{Z}_{15}\times\mathbf{Z}_{36}\\&\cong\mathbf{Z}_5\times(\mathbf{Z}_3\times\mathbf{Z}_5)\times(\mathbf{Z}_4\times\mathbf{Z}_9)\\&\cong\mathbf{Z}_{2^2}\times\mathbf{Z}_3\times\mathbf{Z}_{3^2}\times\mathbf{Z}_5\times\mathbf{Z}_5,\end{aligned}$$
因此 G 的初等因子是
$$\{2^2,3,3^2,5,5\}.$$

初等因子为
$$(p,p,\cdots,p)$$
的 abel p - 群，称为**初等 abel p - 群**(elementary abelian p - group).

对于有限生成的 abel 群的结构有下述结果：

定理 4　设 G 是有限生成的 abel 群，则
$$G\cong\mathbf{Z}_{p_1^{k_{11}}}\times\cdots\times\mathbf{Z}_{p_1^{k_{1r_1}}}\times\cdots\times\mathbf{Z}_{p_s^{k_{s1}}}\times\cdots\times\mathbf{Z}_{p_s^{k_{sr_s}}}\times\mathbf{Z}^t,\quad(28)$$
其中 $p_1,\cdots,p_s$ 是两两不同的素数，$k_{i1}\leqslant k_{i2}\leqslant\cdots\leqslant k_{ir_i}$，$i=1,2,\cdots,s$；$\mathbf{Z}^t\xlongequal{\text{def}}\underbrace{\mathbf{Z}\times\mathbf{Z}\times\cdots\times\mathbf{Z}}_{t\text{个}}$. 我们把(28)式中出现的有限循环群的阶组成的有重集合
$$\{p_1^{k_{11}},\cdots,p_1^{k_{1r_1}},\cdots,p_s^{k_{s1}},\cdots,p_s^{k_{sr_s}}\}$$
称为 G 的**初等因子**；把(28)式中出现的 t 称为 G 的**秩**(rank).

定理 5　两个有限生成的 abel 群同构当且仅当它们有相同的初等因子和相同的秩.

如果一个群 G 同构于 $\mathbf{Z}^t$，则 G 称为秩 t 的**自由 abel 群**(free abelian group). 显然，自由 abel 群中没有有限阶元.

例 3　证明：实数乘法群 $\mathbf{R}^*$ 的有限生成的非平凡子群同构于 $\mathbf{Z}_2$，或者同构于 $\mathbf{Z}^t$，或者同构于 $\mathbf{Z}_2\times\mathbf{Z}^t$，其中 t 是某个正整数.

证明　设 $a\in\mathbf{R}^*$ 是 m 阶元素，则 $a^m=1$，当 m 为奇数时，r^m

1 在 $\mathbf{R}$ 中只有一个解：$x=1$；当 m 为偶数时，$x^m=1$ 在 $\mathbf{R}$ 中恰有两个解：$x=1$ 或 -1. 因此 $\mathbf{R}^*$ 中有限阶元素只有 1 和 -1，其中 -1 是 2 阶元. 由定理 4 即得结论. ┘

习题 1.7

1. 决定 12 阶 abel 群的互不同构的类型.

2. 决定 108 阶 abel 群的互不同构的类型.

3. 决定 360 阶 abel 群的互不同构的类型.

4. 决定 144 阶 abel 群的互不同构的类型.

5. 决定 216 阶 abel 群的互不同构的类型.

6. 求下列群的初等因子：

(1) $\mathbf{Z}_{10}\times\mathbf{Z}_{15}\times\mathbf{Z}_{20}$；

(2) $\mathbf{Z}_{28}\times\mathbf{Z}_{42}$；

(3) $\mathbf{Z}_{9}\times\mathbf{Z}_{14}\times\mathbf{Z}_{6}\times\mathbf{Z}_{16}$.

*7. 设 G 是 100 阶 abel 群.

(1) 证明 G 必含有 10 阶元；

(2) G 的初等因子应当怎样才能使 G 不含阶大于 10 的元素？

*8. 证明：如果有限 abel 群的阶没有平方因子，则它必为循环群.

*9. 证明：一个 abel p - 群如果恰好含有 $p-1$ 个 p 阶元，则它一定是循环群.

*10. 设 V 是域 $\mathbf{Z}_2$ 上的 n 维线性空间，决定 V 的加法群的结构，写出它的初等因子，它是不是初等 abel 2 - 群？

*11. 设 V 是域 $\mathbf{Z}_p$ 上的 n 维线性空间，p 是素数. V 的加法群是不是初等 abel p - 群？

§8 自由群,群的表现

我们已知知道,由一个元素生成的群是循环群.无限循环群都同构于整数加群 $\mathbf{Z}$,有限 m 阶循环群都同构于 $\mathbf{Z}_m$.从 §4 的例 1 知道,对一切正整数 m,$\mathbf{Z}_m$ 是 $\mathbf{Z}$ 的同态像.于是由一个元素生成的群都是 $\mathbf{Z}$ 的同态像.这表明:只要抓住 $\mathbf{Z}$,就可刻画所有的由一个元素生成的群.自然要问:抓住什么样的群,才能刻画所有的多个元素生成的群?

让我们先来分析 $\mathbf{Z}$ 的特征,$\mathbf{Z}$ 的生成元 1 具有如下性质:对一切非零整数 m,都有 $m1 \neq 0$,即生成元 1 只适合平凡的关系:1 的 0 倍等于 0.

一般地,设 X 是群 G 的一个生成元集,如果 X 的元素只适合平凡的关系,即,对于任意 $x_1, x_2, \cdots, x_t \in X$,如果 $x_i \neq x_{i+1}(1 \leqslant i < t)$,并且 $m_1, m_2, \cdots, m_t$ 全不为 0,则

$$x_1^{m_1} x_2^{m_2} \cdots x_t^{m_t} \neq e, \tag{1}$$

则称 X 是群 G 的一个**自由生成元集**(free set of generators).

定义 1 如果群 G 有一个自由生成元集,则称 G 是**自由群**(free group).

例如,$\mathbf{Z}$ 是自由群.因为 $\mathbf{Z}$ 有一个自由生成元素$\{1\}$,所以 $\mathbf{Z}$ 是由一个元素生成的自由群.

如何构造由多个元素生成的自由群?

设 X 是一个非空集合,称 X 是一个字母表.现在我们来构造由 X 生成的自由群.

设 $x_1, x_2, \cdots, x_k \in X$, $m_i \in \mathbf{Z}, 1 \leqslant i \leqslant k$,则

$$x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} \tag{2}$$

称为一个**字**(word).

一个字 $x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}$ 称为**既约的**(reduced),如果 $x_i \neq x_{i+1}$, $1 \leqslant$

$i < k$,并且所有 $m_i \neq 0, 1 \leqslant i \leqslant k$.我们把 x_i^0 也称为既约字.

每一个字都能按照下述规则化简成既约字:如果相邻的两个字母相同,则可合并写成一个字母的方幂,将指数的和作为指数;零次幂省略不写.例如,设 $X = \{x, y, z\}$,则

$$\begin{aligned} w &= x^{-5}x^3y^2y^{-2}x^{-1}xzy^{-1} \\ &= x^{-2}y^0x^0zy^{-1} = x^{-2}zy^{-1}. \end{aligned}$$

我们在下面的定理 1 将证明:每一个字能化简成**唯一**的既约字.

既约字 x_i^0 给出了一个没有任何符号的字(因为 x_i^0 省略不写),我们称它为**空字**(empty word).

两个字相乘就是在第一个字后面接着写第二个字.

字母表 X 形成的所有既约字组成的集合记成 $F(X)$.在 $F(X)$ 中规定乘法运算如下:设 $w_1, w_2 \in F(X)$,则 w_1 与 w_2 的乘积就是在 w_1 后面接着写 w_2,然后把它化简成既约字,例如,设 $w_1 = x^{-2}zy^{-1}, w_2 = yz^{-1}x^7y$,则

$$\begin{aligned} w_1w_2 &= x^{-2}zy^{-1}yz^{-1}x^7y = x^{-2}zz^{-1}x^7y \\ &= x^{-2}x^7y = x^5y. \end{aligned}$$

我们把 w_1w_2 化简成的既约字记成 $\overline{w_1w_2}$.

结合律成立,这是因为 $\overline{(\overline{w_1w_2})w_3}$ 与 $\overline{w_1(\overline{w_2w_2})}$ 是同一个字 $w_1w_2w_3$ 用两种不同方式化简成的既约字 $\overline{w_1w_2w_3}$.

空字是单位元素.

既约字 $x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}$ 的逆是 $x_k^{-m_k}\cdots x_2^{-m_2}x_1^{-m_1}$,它也是既约字.

因此从字母表 X 形成的所有既约字组成的集合 $F(X)$ 成为一个群,容易看出,X 是群 $F(X)$ 的一个自由生成元集.因此 $F(X)$ 是自由群,称它是**由 X 生成的自由群**(free group generated by X).

定理 1 每一个字能化简成唯一的既约字.

证明 设由非空集合 X 形成的所有既约字组成的集合为 Ω,对于 $x \in X$,用下述方式可定义 Ω 的一个置换 σ_x:

$$\sigma_x(w) \xlongequal{\text{def}} \overline{xw}, \quad \forall w \in \Omega. \tag{3}$$

因为 w 是既约字，因此由(3)式定义的 σ_x 是 Ω 到自身的双射，从而 σ_x 是 Ω 的一个置换. 对于任意一个字

$$u = x_1^{n_1} x_2^{n_2} \cdots x_t^{n_t} \tag{4}$$

规定

$$\sigma_u \xlongequal{\text{def}} \sigma_{x_1}^{n_1} \sigma_{x_2}^{n_2} \cdots \sigma_{x_t}^{n_t}. \tag{5}$$

令

$$H = \{\sigma_w \mid w \in \Omega\}, \tag{6}$$

则容易看出，H 对于置换的乘法成为一个群，并且如果一个字 u 化简成既约字 w，则 $\sigma_u = \sigma_w$.

设同一个字 u 用两种不同的方式化简成既约字 w_1, w_2，则据上述结果，有 $\sigma_{w_1} = \sigma_u = \sigma_{w_2}$. 由于 σ_{w_1} 把空字映成 w_1，σ_{w_2} 把空字映成 w_2. 因此 $w_1 = w_2$. □

由一个元素生成的自由群是无限循环群. 由两个或两个以上元素生成的自由群一定是非交换群（因为假如它是 abel 群，则生成元 x_1, x_2 有非平凡的关系 $x_1 x_2 x_1^{-1} x_2^{-1} = e$），并且它的每个非单位元都是无限阶元素.

如果两个非空集合 X 与 Y 之间有一个双射 ψ，则它可诱导自由群 $F(X)$ 到 $F(Y)$ 的一个同构：把 $F(X)$ 的既约字 $x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k}$ 对应于 $F(Y)$ 的既约字 $\psi(x_1)^{m_1} \psi(x_2)^{m_2} \cdots \psi(x_k)^{m_k}$. 我们用 F_n 代表由 n 个元素生成的自由群.

为了说明由 X 生成的自由群 $F(X)$ 处于像 $\mathbf{Z}$ 这种地位，我们先来证明一个结论：

定理 2 设 X 是一个非空集合，G 是一个群. 则 X 到 G 的每一个映射 f 都能唯一地扩充成自由群 $F(X)$ 到 G 的一个同态 φ. 如图 1－8 所示.

证明 定义 $F(X)$ 到 G 的一个对应法则 φ，它把每一个既约字

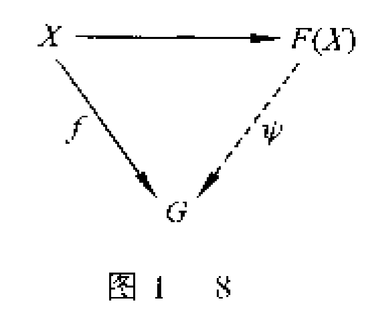


图1-8

$x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}$ 对应到 G 的一个元素

$$[f(x_1)]^{m_1}[f(x_2)]^{m_2}\cdots[f(x_k)]^{m_k}.$$

显然 ψ 是映射,容易看出,ψ 保持运算.因此 ψ 是同态.

唯一性,假如还有 $F(X)$ 到 G 的一个同态 φ 也是由 f 扩充而得到的,则 $\varphi(x)=f(x)=\psi(x)$,$\forall x\in X$.从而对于每一个既约字 $x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}$,有

$$\begin{aligned}\varphi(x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}) &= [\varphi(x_1)]^{m_1}[\varphi(x_2)]^{m_2}\cdots[\varphi(x_k)]^{m_k}\\ &= [\psi(x_1)]^{m_1}[\psi(x_2)]^{m_2}\cdots[\psi(x_k)]^{m_k}\\ &= \psi(x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k}).\end{aligned}$$

因此 $\varphi=\psi$.

定理 3 设 X 是群 G 的一个生成元集,则 G 是自由群 $F(X)$ 的一个同态像.从而 G 同构于自由群 $F(X)$ 的一个商群.

证明 在定理2中取 f 是 X 到 G 的恒等映射,即 $f(x)=x$,$\forall x\in X$.则据定理2得,f 能唯一地扩充成 $F(X)$ 到 G 的一个同态 ψ.现在来证 ψ 是满射.因为 $G=\langle X\rangle$,所以 G 中每一个元素可表示成

$$x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}, \tag{7}$$

其中 $x_i\neq x_{i+1}$,$1\leqslant i<t$,并且所有的 $n_i\neq 0$.于是(7)式是由字母表 X 形成的一个既约字,它属于 $F(X)$.显然有

$$\psi(x_1^{n_1}x_2^{n_2}\cdots x_t^{n_t}) = [f(x_1)]^{n_1}[f(x_2)]^{n_2}\cdots[f(x_t)]^{n_t}$$

$$= x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r}, \tag{8}$$

因此 ψ 是满射. 从而 ψ 是满同态. 这表明 G 是 $F(X)$ 的一个同态像. 从而 G 同构于 $F(X)$ 的一个商群. □

定理 3 表明,任何一个群都是某一个自由群的同态像. 因此只要把握住了所有自由群,就可刻画所有的群.

定理 3 指出,设 X 是群 G 的一个生成元集,则 G 是自由群 $F(X)$ 的一个同态像. 用 N 表示这个同态 ψ 的核,则

$$F(X)/N \cong G.$$

设 R 是 $F(X)$ 的一个子集,如果 R 生成的正规子群是 N(即,包含 R 的所有正规子群的交是 N),则 R 里的字恰好决定了 $F(X)$ 里的哪些字在同态 ψ 下映成了 G 的单位元,我们称 R 是 G 的**一组定义关系**(a set of defining relations).

例如,D_n 的一个生成元集是 $X = \{\sigma, \tau\}$. 可以证明 $\{\sigma^n, \tau^2, (\sigma\tau)^2\}$ 是 D_n 的一组定义关系. 证明如下:

设 M 是 $F(X)$ 中由 $\{\sigma^n, \tau^2, (\sigma\tau)^2\}$ 生成的正规子群. 用 N 表示从 $F(X)$ 到 D_n 的同态 ψ 的核. 我们要证 $M = N$. 从定理 3 的证明过程看到,$\psi(\sigma^n) = \sigma^n = e, \psi(\tau^2) = \tau^2 = e, \psi((\sigma\tau)^2) = (\sigma\tau)^2 = e$,因此 $[\sigma^n, \tau^2, (\sigma\tau)^2] \subseteq N$. 从而 $M \subseteq N$. 于是据 §4 的第二同构定理得,

$$(F(X)/M)\big/(N/M) \cong F(X)/N \tag{9}$$

又由于 $F(X)/N \cong D_n$,因此 $|F(X)/M| \geqslant |D_n| = 2n$.

显然 $F(X)/M = \langle \sigma M, \tau M \rangle$,并且它们满足

$$(\sigma M)^n = \sigma^n M = M, \quad (\tau M)^2 = M, \quad (\sigma\tau M)^2 = M,$$

或者等价地

$$(\sigma M)^n = M, \quad (\tau M)^2 = M, \quad (\tau\sigma) M = \sigma^{n-1}\tau M. \tag{10}$$

从(10)式得出,$F(X)/M$ 中每一个元素属于下述集合:

$$\{M, \sigma M, \cdots, \sigma^{n-1}M, \tau M, \sigma\tau M, \cdots, \sigma^{n-1}\tau M\}.$$

从而 $|F(X)/M| \leq 2n$. 综上述得, $|F(X)/M| = 2n$. 从(9)式得, $|N/M| = 1$, 即 $N = M$. 因此 $\{\sigma^n, \tau^2, (\sigma\tau)^2\}$ 是 D_n 的一组定义关系. □

定义 2 设 X 是一个非空集合, R 是自由群 $F(X)$ 的一个非空子集. 用 N 表示 R 生成的正规子群(即, $F(X)$ 中包含 R 的所有正规子群的交), 则商群 $F(X)/N$ 称为是由**生成元集 X 和定义关系集 R 决定的群**. 如果群 G 同构于 $F(X)/N$, 则 X, R 称为 G 的一个**表现**(presentation), 记作 $G \cong \{X|R\}$. 特别地, 如果 $X = \{x_1, \cdots, x_s\}$, 并且 $R = \{w_1, \cdots, w_t\}$, 那么我们称 G 是**有限表现的**(finitely presented), 记作

$$G \cong \{x_1, \cdots, x_s | w_1, \cdots, w_t\}. \tag{11}$$

例如,

$$\mathbf{Z} \cong \{x | -\}; \quad \mathbf{Z}_m \cong \{x | x^m\};$$

$$D_n \cong \{x, y | x^n, y^2, (xy)^2\};$$

$$Q \cong \{x, y | x^4, x^2y^{-2}, xyxy^{-1}\};$$

$$\mathbf{Z} \times \mathbf{Z} \cong \{x, y | xyx^{-1}y^{-1}\};$$

表现 $\{x_1, \cdots, x_n | x_i x_j x_i^{-1} x_j^{-1}, 1 \leq i \leq j \leq n\}$ 决定了一个秩 n 的自由 abel 群.

同一个群可以有许多不同的表现. 例如

$$\mathbf{Z}_6 \cong \{x | x^6\} \cong \{x, y | x^2, y^3, xyx^{-1}y^{-1}\},$$

$\mathbf{Z}_6$ 的第二种表现描述了 $\mathbf{Z}_6$ 的另一种形式: $\mathbf{Z}_2 \times \mathbf{Z}_3$.

用生成元和定义关系表现群的理论称为**组合群论**(Combinatorial Group Theory). 近几年, 组合群论被用来构造公钥密码系统(参看 M. Anshel, Constructing puplic key cryptosystems via combinatorial group theory, Cryptography – Research Digest 862, Vol. 1 (Nov. 15, 1999)).

如果群 G 是有限表现的, 并且它有一个形如(11)式的表现, 其

中$\{x_1,\cdots,x_s\}$是G的一个生成元集,则也可以把G记作

$$G=\langle x_1,\cdots,x_s\,|\,w_1=e,\cdots,w_t=e\rangle, \qquad (12)$$

其中$w_1=e,\cdots,w_t=e$是生成元$x_1,\cdots,x_s$的一组关系.习惯上,把(12)式也叫做G的一个表现(presentation).

例如,$\mathbf{Z}_m=\langle\bar{1}\,|\,m\bar{1}=\bar{0}\rangle$;

$$D_n=\langle\sigma,\tau\,|\,\sigma^n=I,\tau^2=I,(\sigma\tau)^2=I\rangle;$$

$$Q=\langle \boldsymbol{i},\boldsymbol{j}\,|\,\boldsymbol{i}^4=1,\boldsymbol{i}^2\boldsymbol{j}^{-2}=1,\boldsymbol{i}\boldsymbol{j}\boldsymbol{i}\boldsymbol{j}^{-1}=1\rangle.$$

现在我们利用群的表现这一概念来介绍辫群,它首先由Aritin于1947年提出.辫群在数学物理,低维拓朴,组合群论和表示论中起着重要作用.近几年,辫群被用来构造公钥密码系统和密钥交换协议(参看K.H.KO,S.J.Lee,J.H.Cheon,J.W.Han,J.S.Kang,and C.Park,New public-key cryptosystem using braid groups,CRYPTO 2000,Lecture Notes in Computer Science 1880,ed.M:Bellare,Springer-Verlag(2000),166-183).

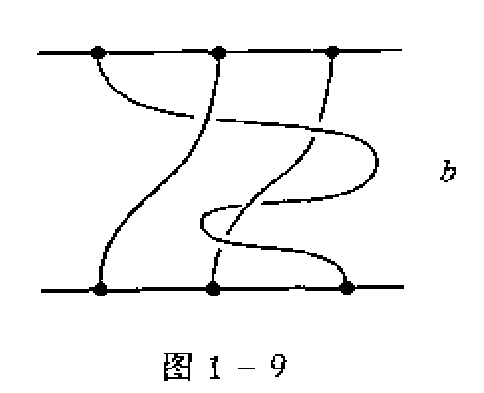


图1-9

给了两个水平平面,在顶面有三个点,它们分别在底面有正投影.把顶面的三个点与它们在底面的正投影的三个点分别用三根绳子连接起来,如图1-9所示,这三根绳子必须不相交,并且每一根绳子与这两个平面之间的每一个水平面恰好相交一次,这样的三根绳子称为一个3-**辫子**(braid),其中3称为**辫指数**(braid intex).

给了两个3-辫子b_1,b_2,它们可以做乘法:b_1b_2就是把b_2放在

b_1 下面得到的辫子,如图 1－10 所示.

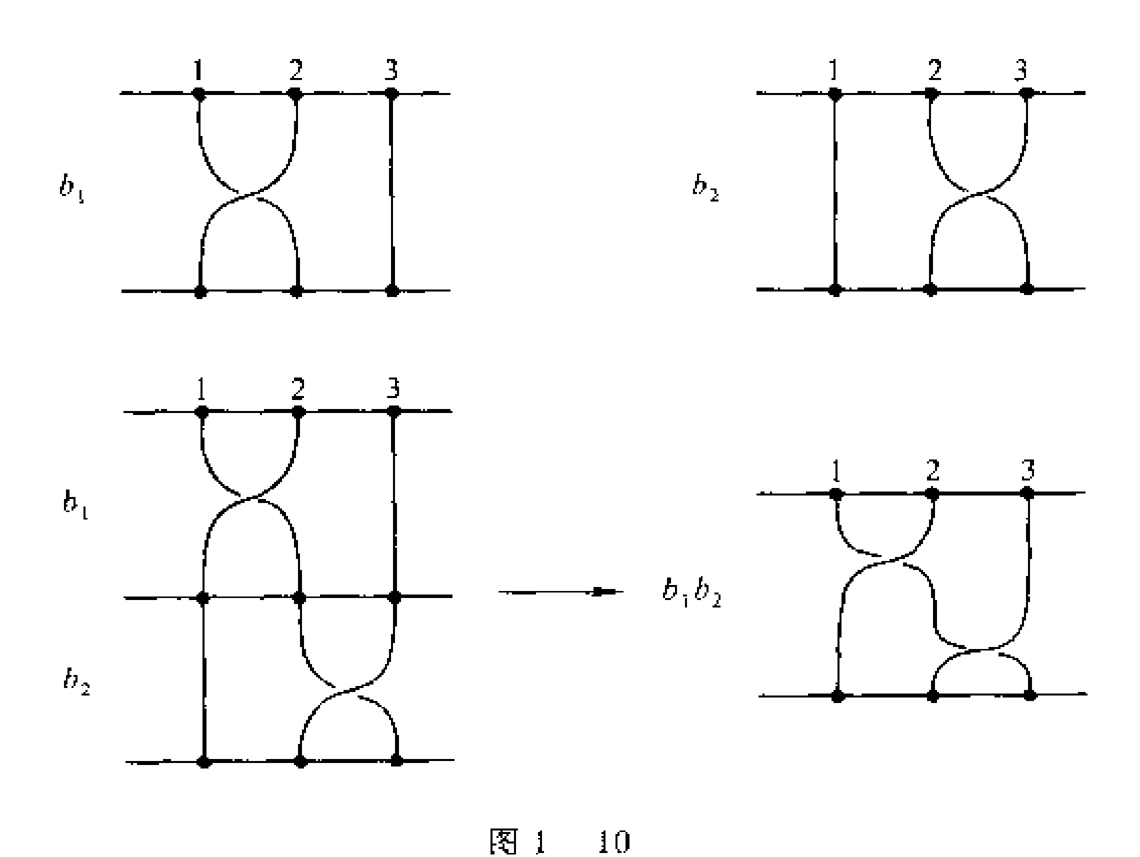


图 1－10

3 根铅直的绳子组成的辫子称为平凡的辫子,用 e 表示,一个辫子的本质是它的绳子彼此缠绕的方式,因此平凡的辫子 e 在上述乘法中起着单位元素的作用,如图 1－11 所示,其中 b 是图 1－9 中所画.

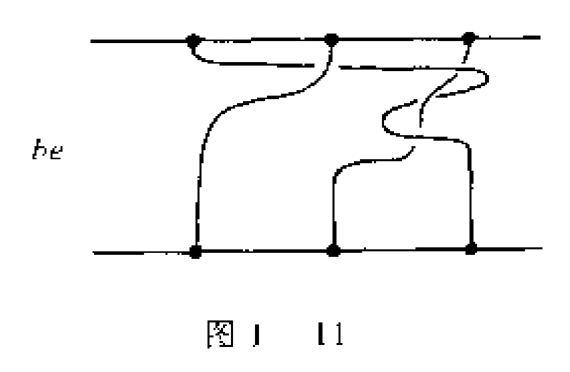
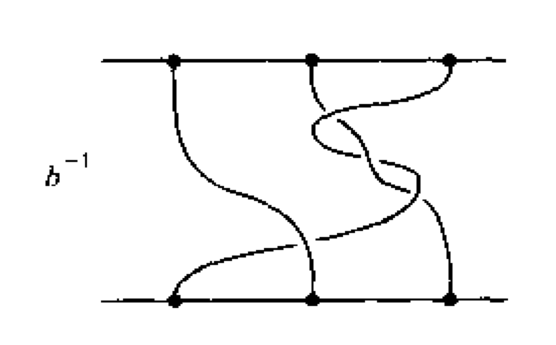


图 1－11

辫子 b 在关于底面的镜面反射下的像给出了一个辫子，记作 b^{-1}. 注意 bb^{-1} 实质上是平凡的辫子，如图 1 - 12 所示，在 bb^{-1} 中，绳子 BB' 在最前面，绳子 AA' 扯直以后在中间，绳子 CC' 扯直以后在最后面. 因此 bb^{-1} 实质上是平凡的辫子，读者不妨动手试一试.



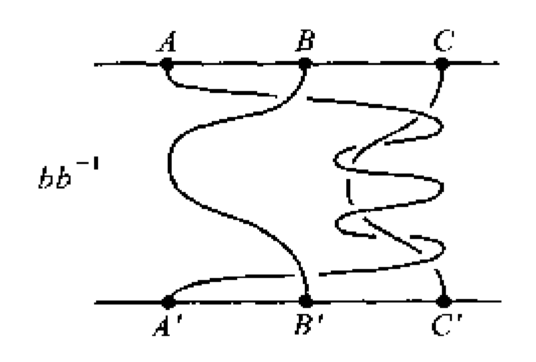


图 1 - 12

从 bb^{-1} 实质上是平凡辫子的议论中看到，我们把一个辫子与经过扯直以后得到的辫子看成实质上是同一个辫子. 精确地说，我们在所有 3 - 辫子组成的集合中，定义一个二元关系：$b_1 \sim b_2$ 当且仅当 b_1 能经过连续变形变成 b_2，在变形中，绳子必须位于两个水平平面之间，它们的端点应当保持固定，并且它们不允许相交. 容易看出，$\sim$ 是一个等价关系. 利用辫子的乘法可以定义等价类的乘法：

$$\bar{a}\,\bar{b} \xlongequal{\text{def}} \overline{ab}. \tag{13}$$

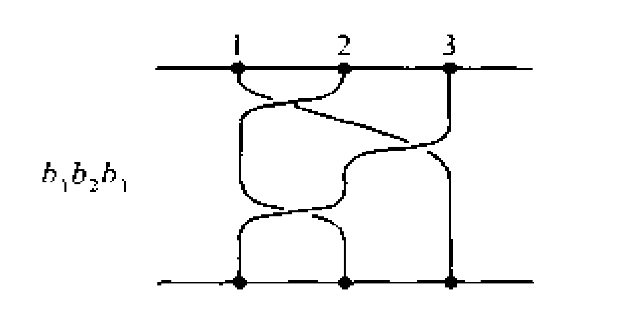
容易看出，(13) 式与等价类的代表的选择无关，因此它的确是等价类的运算. 容易验证，所有等价类组成的集合在这个乘法运算下成为一个群，称它为 3 - **辫群**(braid group)，记作 B_3.

今后我们把 $\bar{b}$ 简单地记成 b.

图 1 - 10 所示的两个 3 - 辫子 b_1, b_2 称为**初等辫子**(elementary braids). 我们来求 $b_1b_2b_1$ 和 $b_2b_1b_2$，如图 1 - 13 所示：

从图 1 - 13 看出

$$b_1b_2b_1 = b_2b_1b_2. \tag{14}$$



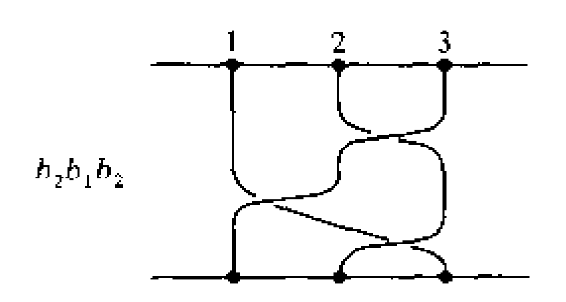


图 1－13

女同志编辫子，用三股头发，两股两股地编．从这不难看出：$\{b_1, b_2\}$ 是 3－辫群 B_3 的一个生成元集，(14) 式是生成元 b_1、b_2 的一组关系．因此 B_3 有一个表现：

$$B_3 = \langle b_1, b_2 \mid b_1b_2b_1 = b_2b_1b_2 \rangle. \tag{15}$$

容易看出，B_3 是无限非交换群．

以上讨论对于 n 条绳子的辫子也成立，从而得到 n－辫群，记作 B_n．n－辫群的初等辫子有 $n-1$ 个：b_i，$1 \leqslant i < n$．如图 1－14 所示．

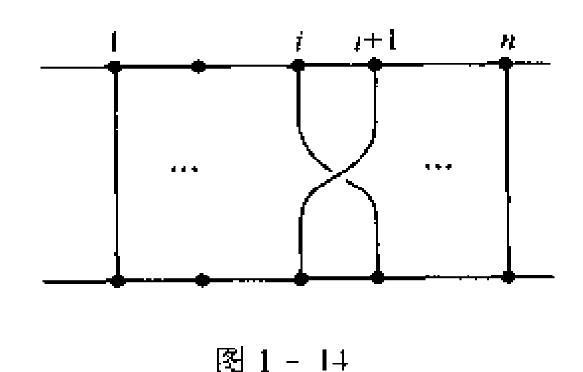


图 1－14

$\{b_1, b_2, \cdots, b_{n-1}\}$ 是 n－辫群 B_n 的一个生成元集．B_n 的一个表现是

$$B_n = \left\langle b_1, \cdots, b_{n-1} \,\middle|\, \begin{array}{ll} b_ib_jb_i = b_jb_ib_j & 当\ |i-j| = 1, \\ b_ib_j = b_jb_i & 当\ |i-j| \geqslant 2 \end{array} \right\rangle. \tag{16}$$

B_n 是无限非交换群．

在 B_3 的构造中，包括了一对水平平面，顶面的三个点和它们在底面

的正投影的三个点.用 1,2,3 分别表示顶面的三个点以及它们在底面的正投影.沿着一个辫子的三条绳子滑动,产生一个 3 元置换.例如,从 b_1 产生(12),从 b_2 产生(23),从图 1－9 的辫子 b 产生(132).容易看出,用这种方法构造的从 B_3 到 S_3 的映射 ψ 是满射,并且 ψ 保持运算(这时置换的乘法 $\sigma\tau$ 要求先做左边的 σ,后做右边的 τ).因此 ψ 是 B_3 到 S_3 的一个满同态.注意 ψ 决不会是单射,因为 B_3 是无限群,而 S_3 是有限群.

习题 1.8

1. 把下列由字母表 $X = \{x, y, z\}$ 形成的字化简成既约字:

(1) $w_1 = x^{-1}y^4y^{-1}z^{-3}zz^2y^{-1}z^{-2}$;

(2) $w_2 = z^2y^{-3}x^2x^{-2}yx^3z^{-5}z^3$;

(3) $w_3 = z^2yx^4x^{-3}x^{-1}z^4y^2zz^{-1}y^{-3}$.

2. w_1, w_2, w_3 同第 1 题,求 $\overline{w_1w_2}, \overline{w_1}\,\overline{w_2w_3}$.

*3. 证明

(1) $S_4 \equiv \{a, b \mid a^2, b^4, (ab)^3\}$;

(2) $S_4 \equiv \{a, c \mid a^2, c^3, (ac)^4\}$.

*4. 证明:$A_4 \equiv \{a, b \mid a^2, b^3, (ab)^3\}$.

*5. 在 3－辫群 B_3 中,求 $b_1^2, b_1b_2b_1^2$,其中 b_1, b_2 是初等辫子(见 §8 的图 1－10).

*6. 在 3－辫群 B_3 中,分别写出 $b_1^2, b_1b_2b_1^2$ 产生的 S_3 中的置换.

*7. 找出 B_3 中的两个不同的辫子,它们都产生置换(132).

*8. 在 4－辫群 B_4 中,求 b_1b_3 和 b_3b_1,其中 b_1, b_3 都是初等辫子(见 §8 的图 1－14).从所画的图看,b_1b_3 与 b_3b_1 相等吗?

*9. 设 G 和 G' 是两个群.$x_1x_2\cdots x_n$ 称为一个**字**,其中每个 x_i 属于无交并 $G \dot{\cup} G'$(即,把 G 的元素与 G' 的元素看成不同的元素形成的并集,注意即使 $G = G'$,在求无交并 $G \dot{\cup} G'$ 时,也需要把前一个集合 G 与后

一个集合 G 的元素看成不同的元素). 称一个字是既约的如果 x_i 与 x_{i+1} 不在同一个群里($1 \leqslant i < n$), 并且 x_i 不是 G 或 G' 的单位元($1 \leqslant i \leqslant n$). 可证每一个字能化简成唯一的既约字(类似于本节定理 1 的证法). 两个既约字 w_1 与 w_2 相乘就是在 w_1 后面接着写 w_2, 然后把它化简成既约字. 所有既约字连同空字组成的集合对于上述乘法成一个群, 称它为 G 与 G' 的**自由积**(free product), 记作 $G * G'$.

证明: $\mathbf{Z} * \mathbf{Z} \cong F_2$, 其中 F_2 代表由 2 个元素生成的自由群.

第二章　环

§1　环的类型和性质,理想

我们已知知道,**环** R 是定义了加法、乘法两个代数运算的非空集合,并且 R 对于加法成一个 abel 群,R 的乘法满足结合律,以及乘法对加法的左、右分配律.

如果环 R 的乘法还适合交换律,则称 R 为**交换环**.

如果环 R 有一个元素 e 具有性质:

$$ae = ea = a, \quad \forall a \in R, \tag{1}$$

则称 e 是 R 的**单位元素**;此时称 R 是**有单位元的环**,R 的单位元素是唯一的,通常把单位元记成 1.

在有单位元的环 R 中,对于元素 a,如果 R 中有元素 b,使得

$$ab = ba = 1, \tag{2}$$

则称 a 是**可逆元**或**单位**,称 b 是 a 的**逆元**,a 的逆元是唯一的,记成 a^{-1}.

环 R 中的元素 a 称为一个**左(或右)零因子**(left (right) zero divisor),如果 R 中有元素 $b \neq 0$,使得 $ab = 0$(或 $ba = 0$).左零因子和右零因子都简称为**零因子**.0 是平凡的零因子;其余的零因子称为**非平凡的零因子**.如果环 R 没有非平凡的零因子,则称 R 是**无零因子环**.

有单位元 $1(\neq 0)$ 的无零因子的交换环称为**整环**(commutative domain).

环 R 称为**除环**(division ring)或**体**,如果 R 的所有非零元组成的集合 R^* 对于乘法成一个群(也就是说,R 是一个有单位元 $1(\neq 0)$ 的环,并且 R 的每一个非零元都可逆).

交换除环称为**域**(field)．即，如果 F 是一个有单位元 $1(\neq 0)$ 的交换环，并且它的每一个非零元都可逆，则称 F 是一个域．

我们已经知道的具体的环有：整数环 $\mathbf{Z}$，域 F 上的 n 级全矩阵环 $M_n(F)$，域 F 上的一元多项式环 $F[x]$，域 F 上的 n 元多项式环 $F[x_1, x_2, \cdots, x_n]$，模 m 剩余类环 $\mathbf{Z}_m$ 等．

1843 年，哈密顿(Hamilton) 发现了**四元数**(quaternion)：

$$a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}, \tag{3}$$

其中 a,b,c,d 为实数，$\boldsymbol{i},\boldsymbol{j},\boldsymbol{k}$ 满足

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \tag{4}$$

$$\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}, \quad \boldsymbol{jk} = -\boldsymbol{kj} = \boldsymbol{i},$$

$$\boldsymbol{ki} = -\boldsymbol{ik} = \boldsymbol{j}. \tag{5}$$

所有四元数组成的集合用 $\boldsymbol{H}$ 表示，规定 $\boldsymbol{H}$ 的加法类似于复数的加法，乘法类似于复数的乘法，则容易验证 $\boldsymbol{H}$ 成为一个除环，称它为**四元数除环**或**四元数体**(quaternion field)．$\boldsymbol{H}$ 是非交换的除环．

如果环 R 的一个非空子集 R_1 对于 R 的加法和乘法也成为一个环，则称 R_1 是 R 的一个**子环**(subring)．

容易证明：环 R 的一个非空子集 R_1 为一个子环的充分必要条件是，R_1 对于 R 的减法与乘法都封闭，即

$$a,b \in R_1 \Longrightarrow a - b \in R_1, \quad ab \in R_1.$$

现在我们来看环的简单性质，设 R 是一个环．

由于 R 对于加法成为一个 abel 群，于是可定义任一元素 a 的"倍数"：对于 $n \in \mathbf{Z}^+$，$0 \in \mathbf{Z}$，规定

$$na \xlongequal{\text{def}} \underbrace{a + a + \cdots + a}_{n\text{个}},$$

$$0a \xlongequal{\text{def}} 0 \quad (\text{右边的 } 0 \in R),$$

$$(-n)a \xlongequal{\text{def}} n(-a),$$

并且满足

$$na + ma = (n+m)a, \quad \forall\, n, m \in \mathbf{Z}, \quad a \in R;$$

$$m(na) = (mn)a, \quad \forall\, n, m \in \mathbf{Z}, \quad a \in R;$$

$$n(a+b) = na + nb, \quad \forall\, n \in \mathbf{Z}, \quad a, b \in R.$$

由于 R 的乘法运算满足结合律,因此可定义任一元素 a 的正整数指数幂:对于 $n \in \mathbf{Z}^+$,规定

$$a^n \overset{\text{def}}{=\!=} \underbrace{aa\cdots a}_{n\text{个}},$$

并且满足

$$a^n a^m = a^{n+m}, \quad \forall\, n, m \in \mathbf{Z}^+, \quad a \in R;$$

$$(a^n)^m = a^{nm}, \quad \forall\, n, m \in \mathbf{Z}^+, \quad a \in R.$$

环 R 既有加法,又有乘法,反映加法与乘法的相容关系的性质有

(i) $0a = a0 = 0$, $\forall\, a \in R$,(这里的 $0 \in R$);

(ii) $a(-b) = -ab$, $(-a)b = -ab$,

$(-a)(-b) = ab$, $\forall\, a, b \in R$;

(iii) $(na)b = a(nb) = n(ab)$, $\forall\, a, b \in R, n \in \mathbf{Z}$;

(iv) $\left(\sum\limits_{i=1}^{n} a_i\right)\left(\sum\limits_{j=1}^{m} b_j\right) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} a_i b_j$, $\forall\, a_i, b_j \in R$.

证明　(i) 取 $b \in R$,有

$$ab = a(b+0) = ab + a0.$$

上式两边加上 $(-ab)$,得 $0 = a0$.同理可证,$0a = 0$.

(ii) 因为

$$(-a)b + ab = [(-a) + a]b = 0b = 0,$$

所以 $(-a)b = -ab$.

同理可证,$a(-b) = -ab$.从而

$$(-a)(-b) = -[a(-b)] = -(-ab) = ab.$$

(iii) 设 $n \in \mathbf{Z}^+$,则

$$(na)b = (\underbrace{a + a + \cdots + a}_{n\text{个}})b = \underbrace{ab + ab + \cdots + ab}_{n\text{个}}$$

$$= n(ab);$$

同理可证,$a(nb) = n(ab)$.

$$[(-n)a]b = [n(-a)]b = n[(-a)b] = n(-ab)$$
$$= (-n)(ab);$$

同理可证,$a[(-n)b] = (-n)(ab)$.

$$(0a)b = 0b = 0,\ a(0b) = a0 = 0,$$
$$0(ab) = 0,$$

因此
$$(0a)b = a(0b) = 0(ab).$$

(iv) 由左、右分配律立即得到. □

如果 R 是交换环,则二项式定理成立,即

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

设 $f(x_1, x_2, \cdots, x_n) \in F[x_1, x_2, \cdots, x_n]$,如果

$$\alpha = (c_1, c_2, \cdots, c_n) \in F^n$$

使得 $f(c_1, c_2, \cdots, c_n) = 0$,则称 α 是 $f(x_1, x_2, \cdots, x_n)$ 的一个**零点**(zero point). $f(x_1, x_2, \cdots, x_n)$ 的所有零点组成的集合称为 F^n 的一个**超曲面**(hypersurface),或**仿射超曲面**(affine hypersurface),记作 $V(f)$. 特别地,$n = 2$ 时,$V(f)$ 称为**平面曲线**(plane curve),或**曲线**,或**仿射曲线**;$n = 3$ 时,$V(f)$ 称为**曲面**(surface).

$F[x_1, x_2, \cdots, x_n]$ 中的一组多项式 $\{f_i(x_1, x_2, \cdots, x_n)\}$ 的公共零点集称为 F^n 的一个**代数簇**(algebraic variety),或者**仿射代数簇**(affine algebraic variety),记作 $V(\{f_i\})$,我们也称 $V(\{f_i\})$,是由 $\{f_i\}$ **定义的**.

数学的一个重要分支——代数几何(algebraic geometry) 的主要研究对象就是代数簇. 研究代数簇的关键想法是什么?让我们来看下面的例子.

在几何空间中建立一个直角坐标系 $Oxyz$. 设

$$f_1(x, y, z) = x^2 + y^2 - 1, \quad f_2(x, y, z) = z.$$

则 f_1 与 f_2 的公共零点集是 xOy 平面上的单位圆 C. 因此 C 是一个代数

簇.这里我们是把 C 看成圆柱面 $x^2+y^2-1=0$ 与 xOy 平面 $z=0$ 的交.但是 C 也可以看成是单位球面 $x^2+y^2+z^2-1=0$ 与 xOy 平面的交;C 还可以看成是圆柱面 $x^2+y^2-1=0$ 与单位球面 $x^2+y^2+z^2-1=0$ 的交;等等.这促使我们考虑其零点集包含 C 的所有多项式组成的集合:

$$I=\{f(x,y,z)\in \mathbf{R}[x,y,z]\mid f(c_1,c_2,c_3)=0,\ \forall (c_1,c_2,c_3)\in C\}.$$

环 $\mathbf{R}[x,y,z]$ 的这个子集 I 有什么性质?显然,I 对于多项式的减法封闭,即

$$f(x,y,z)\in I,g(x,y,z)\in I\Longrightarrow f(x,y,z)-g(x,y,z)\in I.$$

此外,I 还有"吸收性",即

$$f(x,y,z)\in I,h(x,y,z)\in \mathbf{R}[x,y,z]\Longrightarrow f(x,y,z)h(x,y,z)\in I.$$

因此 I 是环 $\mathbf{R}[x,y,z]$ 的具有"吸收性"的子环,称 I 是理想子环,简称为理想.

定义 1　设 R 是一个环,I 是 R 的一个非空子集.如果 I 对于减法封闭,即

$$a\in I,\ b\in I\Longrightarrow a-b\in I;$$

并且 I 具有"吸收性",即

$$a\in I,r\in R\Longrightarrow ar\in I,\ ra\in I,$$

则称 I 是 R 的一个**理想**(ideal)或**双边理想**.如果 I 对于减法封闭,并且具有"左(或右)吸收性",即

$$a\in I,r\in R\Longrightarrow ra\in I(\text{或 } ar\in I),$$

则称 I 是 R 的一个**左(或右)理想**(left (or right) ideal).

由于理想(或左理想,右理想)I 对减法封闭,因此 I 是 R 的加法群的子群.

显然,$\{0\}$ 与 R 都是环 R 的理想,称它们为**平凡的理想**.如果环 R 只有平凡的理想,则称 R 是**单环**(simple ring).

从上面的例子看到,在 $\mathbf{R}^3$ 中给了一个代数簇 C,就可以得到环 $\mathbf{R}[x,y,z]$ 的一个理想 I. 反之,给了环 $\mathbf{R}[x,y,z]$ 的一个理想 I,那么 I 中所有多项式的公共零点集就是 $\mathbf{R}^3$ 的一个代数簇. 由此看出,研究 F^n 的代数簇的关键想法是研究环 $F[x_1,x_2,\cdots,x_n]$ 的理想.

理想的理论不仅在代数几何里是至关重要的,而且在环论本身,以及代数数论,代数组合论,编码,密码等领域都起着重要作用.

在整数环 $\mathbf{Z}$ 中,一个整数 m 的所有倍数组成的集合记作 $m\mathbf{Z}$. 容易看出,$m\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个理想.

在域 F 上的一元多项式环 $F[x]$ 中,一个多项式 $f(x)$ 的所有倍式组成的集合是 $F[x]$ 的一个理想.

一般地,设 R 是一个有单位元的交换环,$a \in R$,把集合 $\{ra \mid r \in R\}$ 记作 Ra. 容易看出,Ra 是 R 的一个理想.

容易看出,如果 $\{I_j \mid j \in J\}$ 是环 R 的一族理想,则 $\bigcap_{j \in J} I_j$ 也是 R 的一个理想.

设 S 是环 R 的一个非空子集,环 R 的包含 S 的所有理想的交称为由 S **生成的理想**(ideal generated by S),记作 (S). 如果 $S = \{a_1, a_2, \cdots, a_n\}$,则称 (S) 是**有限生成的**,并且把 (S) 记成 $(a_1, a_2, \cdots, a_n)$.

环 R 中由一个元素 a 生成的理想称为**主理想**(principal ideal),记作 (a).

设 R 是有单位元的交换环. 容易看出 Ra 是由一个元素 a 生成的理想,因此 Ra 是主理想. 于是可把 Ra 记成 (a). 特别地,在整数环 $\mathbf{Z}$ 中,$m\mathbf{Z}$ 是主理想,可记成 (m);在 $F[x]$ 中,一个多项式 $f(x)$ 的所有倍式组成的集合是主理想,可记成 $(f(x))$.

注:设 R 是一个环(不一定有单位元,也不一定是交换环),则一个元素 a 生成的理想 (a) 为

$$(a) = \left\{ r_1 a + a r_2 + m a + \sum_{i=1}^{n} x_i a y_i \mid r_1, r_2, x_i, y_i \in R, \right.$$

$$m \in \mathbf{Z}, n \in \mathbf{Z}^+\}.$$

设 R 是有单位元的交换环，$a_1, a_2, \cdots, a_n \in R$. 容易证明

$$(a_1, a_2, \cdots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_i \in R, \quad i = 1, 2, \cdots, n\}. \tag{6}$$

设 A, B 是环 R 的两个非空子集. 规定

$$A + B \overset{\text{def}}{=\!=} \{a + b \mid a \in A, b \in B\};$$

$$AB \overset{\text{def}}{=\!=} \{a_1b_1 + \cdots + a_nb_n \mid a_i \in A, b_i \in B, i = 1, \cdots, n, n \in \mathbf{Z}^+\}.$$

容易看出，如果 I, J 是环 R 的两个理想，则 $I + J$, IJ 也是环 R 的理想，分别称为 I 与 J 的和，积；并且有

$$IJ \subseteq I \cap J \subseteq I + J. \tag{7}$$

理想的加法，乘法，求交都是理想的运算，容易证明它们满足以下的法则：设 I, J, K 都是环 R 的理想，则

$I + J = J + I$，(加法交换律)；

$(I + J) + K = I + (J + K)$，(加法结合律)；

$(IJ)K = I(JK)$，(乘法结合律)；

$I(J + K) = IJ + IK$，(左分配律)；

$(J + K)I = JI + KI$，(右分配律).

在整数环 $\mathbf{Z}$ 中，容易看出

$$(n)(m) = \{(k_1n)(l_1m) + \cdots + (k_tn)(l_tm) \mid k_i, l_i \in \mathbf{Z}, \quad t \in \mathbf{Z}^+\} = (nm); \tag{8}$$

$$(n) \cap (m) = ([n, m]); \tag{9}$$

$$(n) + (m) = \{kn + lm \mid k, l \in \mathbf{Z}\} = ((n, m)). \tag{10}$$

于是

$$(n, m) = 1 \iff (n) + (m) = (1) = \mathbf{Z}.$$

由此受到启发，我们引出下面的概念：

定义 2 设 R 是有单位元的环，I, J 是 R 的理想. 如果 $I + J =$

R,则称 I 与 J 互素(coprime).

命题 1 设 R 是有单位元的环,I,J,K 都是 R 的理想,如果 I 和 J 都与 K 互素,则 IJ 也与 K 互素.

证明 由于 $I+K=R$,$J+K=R$,因此存在 $a\in I,k_1\in K$,$b\in J,k_2\in K$,使得

$$a+k_1=1,\quad b+k_2=1.$$

上面两个等式的左、右两边分别相乘,得

$$ab+(ak_2+k_1b+k_1k_2)=1.$$

由于 K 是 R 的理想,因此 $ak_2+k_1b+k_1k_2\in K$.而 $ab\in IJ$,因此 $1\in IJ+K$.由于 $IJ+K$ 也是 R 的理想,因此对于任意 $r\in R$,有

$$r=r\cdot 1\in IJ+K.$$

即 $R\subseteq IJ+K$.显然有 $IJ+K\subseteq R$,因此

$$IJ+K=R.$$

这证明了 IJ 与 K 互素. □

命题 2 设 R 是有单位元的交换环,I,J 是 R 的理想,则

$$I\text{ 与 }J\text{ 互素}\Longrightarrow IJ=I\cap J.$$

证明 已经知道,$IJ\subseteq I\cap J$.因此只要证 $I\cap J\subseteq IJ$.因为 I 与 J 互素,所以存在 $a\in I,b\in J$,使得

$$a+b=1.$$

任取 $x\in I\cap J$,用 x 乘上式两边,得

$$xa+xb=x.$$

由于 R 是交换环,因此 $xa=ax$.从而

$$x=ax+xb\in IJ.$$

于是 $I\cap J\subseteq IJ$.因此 $IJ=I\cap J$. □

据命题 2 得,在 $\mathbf{Z}$ 中 n 与 m 互素 $\Longrightarrow (n)(m)=(n)\cap(m)$.

类似于整数环 $\mathbf{Z}$,在域 F 上的一元多项式环 $F[x]$ 中,

$$(f(x))(g(x))=(f(x)g(x));$$

$$(f(x))\cap(g(x))=([f(x),g(x)]);$$

$$(f(x)) + (g(x)) = (f(x), g(x));$$

$f(x)$ 与 $g(x)$ 互素 $\Longleftrightarrow (f(x))$ 与 $(g(x))$ 互素.

据命题 2 得

$f(x)$ 与 $g(x)$ 互素 $\Longrightarrow (f(x))(g(x)) = (f(x)) \cap (g(x))$.

习题 1.2

1. 设 F 是一个域，令

$$S = \{aE_{11} \mid a \in F\},$$

证明 S 是 $M_n(F)$ 的一个子环；并且求 S 的单位元.

2. 证明有限整环一定是域.

*3. 令

$$\mathbf{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbf{C} \right\},$$

证明 $\mathbf{H}$ 是一个除环.

4. 设 R 是有单位元的环，证明 R 的每一个非平凡的理想都不可能含有单位元.

5. 证明域 F 没有非平凡的理想.

6. 设 R 是一个有单位元的交换环，证明：如果 R 没有非平凡的理想，则 R 是一个域.

7. 设 I 是交换环 R 一个理想. 令

$$\mathrm{rad} I = \{r \in R \mid r^n \in I \text{ 对某一正整数 } n\}.$$

证明 $\mathrm{rad} I$ 也是 R 的一个理想. 称 $\mathrm{rad} I$ 是 I 的**根**(radical).

8. 环 R 中元素 a 称为**幂零元**(nilpotent element)，如果有一个正整数 n，使得 $a^n = 0$. 证明：如果 a 是有单位元的环 R 中的一个幂零元，则 $1 - a$ 可逆.

9. 证明：在交换环 R 中，所有幂零元组成的集合是 R 的一个理想，它是(0) 的根，称为 R 的**幂零根**(nilradical).

*10. 设 D 是一个除环,证明 $M_n(D)$ 是单环.

§2 商环,环的同态,环的直和

设 R 是一个环,I 是 R 的一个理想,则 I 是 R 的加法群的子群.由于 R 的加法群是 abel 群,因此 I 是正规子群,从而有商群 R/I,它的元素是 I 的陪集 $r+I$.我们规定

$$(r_1+I)(r_2+I) \xlongequal{\text{def}} r_1r_2+I. \tag{1}$$

设 $r_1+I=r_1'+I$,$r_2+I=r_2'+I$,则

$$-r_1'+r_1\in I,\quad -r_2'+r_2\in I.$$

从而

$$\begin{aligned}-r_1'r_2'+r_1r_2&=r_1r_2-r_1'r_2+r_1'r_2-r_1'r_2'\\&=(r_1-r_1')r_2+r_1'(r_2-r_2')\in I.\end{aligned}$$

因此 $$r_1r_2+I=r_1'r_2'+I.$$

这表明(1)式中定义的陪集的乘法是合理的.

显然,陪集的乘法满足结合律,以及左、右分配律,因此 R/I 成为一个环,称为 R 对于 I 的**商环**(quotient ring).商环 R/I 中的元素 $r+I$ 称为模 I 的**剩余类**(residue class).

容易看出,如果环 R 有单位元 1,则商环 R/I 有单位元 $1+I$;如果 R 是交换环,则商环 R/I 也是交换环.

例如,在整数环 $\mathbf{Z}$ 中,$m\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个理想,因此有商环 $\mathbf{Z}/m\mathbf{Z}$,它的元素是陪集 $k+m\mathbf{Z}$.由于

$$k+m\mathbf{Z}=\{k+ml\mid l\in\mathbf{Z}\}=\bar{k},$$

因此 $\mathbf{Z}/m\mathbf{Z}=\mathbf{Z}_m$,即 $\mathbf{Z}$ 对于 $m\mathbf{Z}$ 的商环 $\mathbf{Z}/m\mathbf{Z}$ 就是模 m 剩余类环 $\mathbf{Z}_m$.由于 $m\mathbf{Z}=(m)$,因此商环 $\mathbf{Z}/m\mathbf{Z}$ 也可以写成 $\mathbf{Z}/(m)$.设 p 为素数,则商环 $\mathbf{Z}/(p)$ 是一个域,它就是模 p 剩余类域 $\mathbf{Z}_p$.

环 R 到商环 R/I 有一个自然的映射 $\pi: r\mapsto r+I$.显然有

$$\pi(r_1+r_2)=(r_1+r_2)+I=(r_1+I)+(r_2+I)$$
$$=\pi(r_1)+\pi(r_2),$$
$$\pi(r_1r_2)=r_1r_2+I=(r_1+I)(r_2+I)=\pi(r_1)\pi(r_2),$$

即映射 π 保持加法和乘法运算.

定义 1　设 R 和 R' 是两个环,如果 R 到 R' 有一个映射 σ 具有性质:对于所有的 $a,b\in R$,有

$$\sigma(a+b)=\sigma(a)+\sigma(b), \tag{2}$$
$$\sigma(ab)=\sigma(a)\sigma(b), \tag{3}$$
$$\sigma(1)=1', \tag{4}$$

则称 σ 是环 R 到 R' 的一个**同态映射**或**同态**.(注:对于没有单位元的环,不要求公式(4)).

设 σ 是环 R 到 R' 的一个同态,如果 σ 是单射(或满射),则称 σ 是环的**单同态**(或**满同态**).

定义 2　设 R 和 R' 是两个环,如果 R 到 R' 有一个双射 σ 满足公式(2)和(3)(即,σ 保持加法和乘法运算),则称 σ 是环 R 到 R' 的一个**同构映射**或**同构**,此时称环 R 与 R' 是**同构的**,记作 $R\cong R'$.

设 σ 是环 R 到 R' 的一个同态.显然 σ 是 R 的加法群到 R' 的加法群的一个同态,因此有

$$\sigma(0)=0',\quad \sigma(-a)=-\sigma(a). \tag{5}$$

σ 作为加法群的同态的核称为**环同态的核**,仍记作 $\operatorname{Ker}\sigma$,即

$$\operatorname{Ker}\sigma=\{a\in R\mid\sigma(a)=0'\}. \tag{6}$$

环同态 σ 的核 $\operatorname{Ker}\sigma$ 不仅是 R 的加法群的子群,而且是环 R 的一个理想,理由如下:任取 $a\in\operatorname{Ker}\sigma$, $r\in R$,有

$$\sigma(ra)=\sigma(r)\sigma(a)=\sigma(r)0'=0'.$$

因此 $ra\in\operatorname{Ker}\sigma$.同理可证 $ar\in\operatorname{Ker}\sigma$.所以 $\operatorname{Ker}\sigma$ 是 R 的一个理想.

环同态 σ 的像 $\operatorname{Im}\sigma$ 不仅是 R' 的加法群的子群,而且是环 R' 的一个子环(因为 $\operatorname{Im}\sigma$ 对于乘法也封闭).如果环 R,R' 分别有单位元 $1,1'$,则 $1'\in\operatorname{Im}\sigma$.

设 σ 是环 R 到 R' 的一个同构，如果 R, R' 分别有单位元 $1, 1'$，则 $\sigma(1) = 1'$. 理由如下：任取 $r' \in R'$，由于 σ 是满射，因此存在 $r \in R$ 使得 $\sigma(r) = r'$. 于是

$$\sigma(1)r' = \sigma(1)\sigma(r) = \sigma(1 \cdot r) = \sigma(r) = r',$$

同理有 $r'\sigma(1) = r'$. 因此 $\sigma(1)$ 是 R' 的单位元. 从而 $\sigma(1) = 1'$.

我们在前面已指出，环 R 到商环 R/I 有一个自然的映射 $\pi: r \to r + I$，它保持加法和乘法运算. 如果 R 有单位元 1，则 $\pi(1) = 1 + I$，它是 R/I 的单位元. 因此 π 是环 R 到商环 R/I 的一个同态，称它是**自然环同态**. 由于 π 也是 R 的加法群到 R/I 的加法群的自然同态，因此 $\mathrm{Ker}\pi = I$. 这表明自然环同态 π 的核等于理想 I.

从上面的讨论知道，环 R 到 R' 的任一同态 σ 的核是 R 的一个理想；环 R 的每一个理想 I 是自然环同态 π 的核，这样我们对理想与环同态的核之间的关系就了如指掌了.

显然，环 R 到商环 R/I 的自然同态 π 是满同态，因此 $\mathrm{Im}\pi = R/I$. 这表明商环 R/I 是环 R 在自然环同态 π 下的像. 反过来，环 R 的任一同态像与 R 对于同态核的商环之间有什么关系？下面的定理回答了这一问题.

定理 1（环同态基本定理） 设 σ 是环 R 到 R' 的一个同态，则同态像 $\mathrm{Im}\sigma$ 同构于商环 $R/\mathrm{Ker}\sigma$，即

$$R/\mathrm{Ker}\sigma \cong \mathrm{Im}\sigma. \tag{7}$$

证明 由于 σ 也是环 R 的加法群到 R' 的加法群的一个同态，因此据群同态基本定理得，商群 $R/\mathrm{Ker}\sigma$ 与 $\mathrm{Im}\sigma$ 同构，它的一个同构映射是

$$\psi: r + \mathrm{Ker}\sigma \longmapsto \sigma(r). \tag{8}$$

只需要再证 ψ 保持乘法. 任取 $r_1 + \mathrm{Ker}\sigma, r_2 + \mathrm{Ker}\sigma \in R/\mathrm{Ker}\sigma$,

$$\psi[(r_1 + \mathrm{Ker}\sigma)(r_2 + \mathrm{Ker}\sigma)] = \psi(r_1 r_2 + \mathrm{Ker}\sigma)$$
$$= \sigma(r_1 r_2) = \sigma(r_1)\sigma(r_2) = \psi(r_1 + \mathrm{Ker}\sigma)\psi(r_2 + \mathrm{Ker}\sigma).$$

因此 ψ 是环 $R/\mathrm{Ker}\sigma$ 到 $\mathrm{Im}\sigma$ 的一个同构映射. 从而环 $R/\mathrm{Ker}\sigma$ 与 $\mathrm{Im}\sigma$ 同构. □

类似于群的第一同构定理和第二同构定理，我们有环的第一同构定理和第二同构定理.

定理 2(第一环同构定理) 设 R 是一个环，I 是 R 的理想，H 是 R 的子环，则 $I+H$ 是 R 的子环，$I\cap H$ 是 H 的理想，并且有环同构：

$$H/I\cap H\cong I+H/I. \tag{9}$$

证明 由群的第一同构定理得，$I+H$ 是 R 的加法群的子群，$I\cap H$ 是 H 的加法群的子群，并且有群同构：

$$H/I\cap H\cong I+H/I,$$

其中同构映射为

$$\psi: h+I\cap H\longmapsto h+I. \tag{10}$$

只需要再证 $I+H$ 对乘法封闭，$I\cap H$ 对于 H 的元素具有吸收性，以及 ψ 保持乘法运算.

任取 $a_1+h_1, a_2+h_2\in I+H$，有

$$(a_1+h_1)(a_2+h_2)=(a_1a_2+a_1h_2+h_1a_2)+h_1h_2\quad\in I+H.$$

任取 $h\in H, a\in I\cap H$，则 $ha\in I\cap H$. 同理 $ah\in I\cap H$.

任取 $h_1+I\cap H, h_2+I\cap H\in H/I\cap H$，有

$$\begin{aligned}\psi[(h_1+I\cap H)(h_2+I\cap H)]&=\psi(h_1h_2+I\cap H)\\&=h_1h_2+I=(h_1+I)(h_2+I)\\&=\psi(h_1+I\cap H)\psi(h_2+I\cap H).\end{aligned}$$

因此 $I+H$ 是 R 的子环，$I\cap H$ 是 H 的理想，ψ 是环同构. □

定理 3(第二环同构定理) 设 R 是一个环，I,J 都是 R 的理想，且 $I\subseteq J$，则 J/I 是 R/I 的理想，并且有环同构：

$$(R/I)/(J/I)\cong R/J. \tag{11}$$

证明 由群的第二同构定理得，J/I 是 R/I 的加法群的子群，并且有群同构：

$$(R/I)/(J/I)\cong R/J,$$

其中同构映射为

$$\psi:(r+I)+J/I\mapsto r+J. \tag{12}$$

只需要再证 J/I 对于 R/I 的元素具有吸收性,以及 ψ 保持乘法运算.

任取 $r+I\in R/I$, $j+I\in J/I$,有

$$(r+I)(j+I)=rj+I\in J/I.$$

同理,

$$(j+I)(r+I)\in J/I.$$

任取 $(R/I)/(J/I)$ 中两个元素:$(r_1+I)+J/I$,$(r_2+I)+J/I$,

$$\begin{aligned}&\psi\{[(r_1+I)+J/I][(r_2+I)+J/I]\}\\=&\ \psi[(r_1+I)(r_2+I)+J/I]\\=&\ \psi[(r_1r_2+I)+J/I]=r_1r_2+J=(r_1+J)(r_2+J)\\=&\ \psi[(r_1+I)+J/I]\psi[(r_2+I)+J/I],\end{aligned}$$

因此 J/I 是 R/I 的理想,ψ 是环同构. □

设 $R_1,R_2,\cdots,R_s$ 都是环,作 $R_1,R_2,\cdots,R_s$ 的加法群的直和 $R_1\oplus R_2\oplus\cdots\oplus R_s$,在这个直和中定义乘法如下:

$$(a_1,a_2,\cdots,a_s)\cdot(b_1,b_2,\cdots,b_s)\overset{\text{def}}{=\!=}(a_1b_1,a_2b_2,\cdots,a_sb_s). \tag{13}$$

显然这样定义的乘法满足结合律,以及左、右分配律,因此 $R_1\oplus R_2\oplus\cdots\oplus R_s$ 成为一个环,称它为环 $R_1,R_2,\cdots,R_s$ **的直和**.它的零元素是$(0,0,\cdots,0)$.如果每个环 R_i 有单位元素 $1_i(i=1,2,\cdots,s)$,则 $R_1\oplus R_2\oplus\cdots\oplus R_s$ 有单位元素$(1_1,1_2,\cdots,1_s)$.如果每个环 R_i 是交换环$(i=1,2,\cdots,s)$,则 $R_1\oplus R_2\oplus\cdots\oplus R_s$ 也是交换环.

令 $R_i'=\{(0,\cdots,0,a_i,0,\cdots,0)\mid a_i\in R_i\}$,$i=1,2,\cdots,s$.容易验证:

(1) R_i' 是 $R_1\oplus R_2\oplus\cdots\oplus R_s$ 的一个理想,$i=1,2,\cdots,s$;

(2) $R_1\oplus R_2\oplus\cdots\oplus R_s=R_1'+R_2'+\cdots+R_s'$;

(3) $R_i' \cap (\sum_{j \neq i} R_j') = (0), i = 1, 2, \cdots, s$;

(4) $R_i' \cong R_i, i = 1, 2, \cdots, s$.

定理 4 设 $I_1, I_2, \cdots, I_s$ 都是环 R 的理想，并且

$$R = I_1 + I_2 + \cdots + I_s, \tag{14}$$

$$I_i \cap (\sum_{j \neq i} I_j) = (0), i = 1, 2, \cdots, s, \tag{15}$$

则(1) 环 R 的每个元素可唯一表成形式

$$x_1 + x_2 + \cdots + x_s, \quad x_i \in I_i, \ i = 1, 2, \cdots, s;$$

(2) 有环同构：

$$R \cong I_1 \oplus I_2 \oplus \cdots \oplus I_s,$$

此时称环 R 是它的理想 $I_1, I_2, \cdots, I_s$ 的**内直和**.

证明 (1) 设 R 中元素 r 有两种表法：

$$r = x_1 + x_2 + \cdots + x_s = y_1 + y_2 + \cdots + y_s, x_i, y_i \in I_i,$$

则

$$x_1 - y_1 = (y_2 - x_2) + \cdots + (y_s - x_s) \in I_1 \cap (\sum_{j=2}^{s} I_j) = (0).$$

因此 $x_1 = y_1$. 类似地可证，$x_2 = y_2, \cdots, x_s = y_s$.

(2) 据第一章 §3 的定理 5，有群同构：

$$R \cong I_1 + I_2 + \cdots + I_s,$$

其中同构映射为

$$\sigma: x_1 + x_2 + \cdots + x_s \longmapsto (x_1, x_2, \cdots, x_s).$$

当 $i \neq j$ 时，有

$$I_i I_j \subseteq I_i \cap I_j \subseteq I_i \cap (\sum_{k \neq i} I_k) = (0).$$

由此推出

$$\sigma[(x_1 + x_2 + \cdots + x_s) \cdot (y_1 + y_2 + \cdots + y_s)]$$
$$= \sigma(x_1 y_1 + x_2 y_2 + \cdots + x_s y_s) = (x_1 y_1, x_2 y_2, \cdots, x_s y_s)$$

$$= (x_1 + x_2 + \cdots + x_s)(y_1 + y_2 + \cdots + y_s)$$
$$= \sigma(x_1 + x_2 + \cdots + x_s)\sigma(y_1 + y_2 + \cdots + y_s).$$

因此 σ 是环同构映射. □

设 I 是环 R 的一个理想. 则 I 是 R 的加法群的子群. 从而对于 a, $b \in R$, 有

$$a + I = b + I \Longleftrightarrow a - b \in I.$$

定义 3 设 I 是环 R 的一个理想, 对于 $a, b \in R$, 如果 $a - b \in I$, 则称 a, b **模 I 同余**(a is congruent to b modulo I), 记作 $a \equiv b \pmod I$.

容易看出, 如果 $a \equiv b \pmod I$, $c \equiv d \pmod I$, 则

$$a + c \equiv b + d \pmod I, \tag{16}$$
$$ca \equiv cb \pmod I, \tag{17}$$
$$ca \equiv db \pmod I. \tag{18}$$

显然, 模 I 同余具有反身性、对称性和传递性, 因此它是 R 的一个等价关系. 容易看出, a 确定的等价类 $\bar{a} = a + I$. 从而 R 对于模 I 同余的商集就是商环 R/I.

定理 5 设 R 是有单位元 $1(\neq 0)$ 的环, 它的理想 $I_1, I_2, \cdots, I_s$ 两两互素, 则

$$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s. \tag{19}$$

证明 令

$$\sigma:\quad R \longrightarrow R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s$$
$$x \longmapsto (x + I_1, x + I_2, \cdots, x + I_s),$$

则

$$\sigma(x + y)$$
$$= ((x + y) + I_1, (x + y) + I_2, \cdots, (x + y) + I_s)$$
$$= ((x + I_1) + (y + I_1), (x + I_2) + (y + I_2), \cdots, (x + I_s)$$
$$+ (y + I_s))$$

$$= (x + I_1, x + I_2, \cdots, x + I_s) + (y + I_1, y + I_2, \cdots, y + I_s)$$
$$= \sigma(x) + \sigma(y),$$
$$\sigma(xy)$$
$$= (xy + I_1, xy + I_2, \cdots, xy + I_s)$$
$$= ((x + I_1)(y + I_1), (x + I_2)(y + I_2), \cdots, (x + I_s)(y + I_s))$$
$$= (x + I_1, x + I_2, \cdots, x + I_s)(y + I_1, y + I_2, \cdots, y + I_s)$$
$$= \sigma(x)\sigma(y),$$

$\sigma(1) = (1 + I_1, 1 + I_2, \cdots, 1 + I_s)$,

因此 σ 是环 R 到 $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s$ 的一个同态.

$$a \in \mathrm{Ker}\sigma \Longleftrightarrow \sigma(a) = (0 + I_1, 0 + I_2, \cdots, 0 + I_s)$$
$$\Longleftrightarrow a + I_j = 0 + I_j, j = 1, 2, \cdots, s$$
$$\Longleftrightarrow a \in I_j, j = 1, 2, \cdots, s$$
$$\Longleftrightarrow a \in I_1 \cap I_2 \cap \cdots \cap I_s.$$

因此 $\mathrm{Ker}\sigma = I_1 \cap I_2 \cap \cdots \cap I_s$. 据环同态基本定理得

$$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong \mathrm{Im}\sigma.$$

下面来证 σ 是满射. 任取

$$(b_1 + I_1, b_2 + I_2, \cdots, b_s + I_s) \in R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s,$$

要证存在 $a \in R$, 使得 $\sigma(a) = (b_1 + I_1, b_2 + I_2, \cdots, b_s + I_s)$, 即

$$a + I_j = b_j + I_j, \quad j = 1, 2, \cdots, s,$$

即
$$a - b_j \in I_j, \quad j = 1, 2, \cdots, s,$$

即
$$a \equiv b_j (\mathrm{mod}\ I_j), \quad j = 1, 2, \cdots, s.$$

由于 $I_1, I_2, \cdots, I_s$ 两两互素, 因此据本章 §1 的命题 1 得, 对于每个 $j \in \{1, 2, \cdots, s\}$, I_j 与 $I_1 \cdots I_{j-1} I_{j+1} \cdots I_s$ 互素, 从而

$$I_j + I_1 \cdots I_{j-1} I_{j+1} \cdots I_s = R. \tag{20}$$

于是存在 $d_j \in I_j$, $e_j \in I_1 \cdots I_{j-1} I_{j+1} \cdots I_s$, 使得

$$d_j + e_j = 1. \tag{21}$$

由于 $d_j = d_j - 0 \in I_j$，因此 $d_j \equiv 0 \pmod{I_j}$. 从而由(21)式得

$$e_j \equiv 1 \pmod{I_j}. \tag{22}$$

对于 $l \neq j$，由于

$$e_j \in I_1 \cdots I_{j-1} I_{j+1} \cdots I_s \subseteq I_1 \cap \cdots \cap I_{j-1} \cap I_{j+1} \cap \cdots \cap I_s \subseteq I_l,$$

因此 $$e_j \equiv 0 \pmod{I_l},\ l = 1, \cdots, j-1, j+1, \cdots, s. \tag{23}$$

令 $$a = \sum_{i=1}^{s} b_i e_i. \tag{24}$$

则 $$a \equiv b_j \pmod{I_j},\ j = 1, 2, \cdots, s. \tag{25}$$

因此 σ 是满射. 从而

$$R/I_1 \cap I_2 \cap \cdots \cap I_s \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s. \qquad \square$$

在上面证明 σ 是满射时，也就证明了下述中国剩余定理：

定理 6(中国剩余定理) 设 R 是有单位元 $1(\neq 0)$ 的环，它的理想 $I_1, I_2, \cdots, I_s$ 两两互素，则对于任意给定的 s 个元素 $b_1, b_2, \cdots, b_s \in R$，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{I_1} \\ x \equiv b_2 \pmod{I_2} \\ \quad \cdots\cdots \\ x \equiv b_s \pmod{I_s} \end{cases}$$

在 R 内必有解；并且如果 a, c 是两个解，则

$$a \equiv c \pmod{I_1 \cap I_2 \cap \cdots \cap I_s}.$$

证明 在上面证明 σ 是满射时，已证明了这个同余方程组在 R 内有解. 现在设 a, c 都是解，则由模 I_j 同余的对称性和传递性得

$$a \equiv c \pmod{I_j}, \quad j = 1, 2, \cdots, s,$$

即 $$a - c \in I_j, \quad j = 1, 2, \cdots, s.$$

因此 $$a - c \in I_1 \cap I_2 \cap \cdots \cap I_s.$$

从而 $$a \equiv c \pmod{I_1 \cap I_2 \cap \cdots \cap I_s}. \qquad \square$$

我国古代韩信点兵问题就是中国剩余定理的一个特殊情况："有

一队士兵，三三数余 2，五五数余一，七七数余四．问：这队士兵有多少人？"

在公钥密码学等领域中，常常要在模 m 剩余类环 $\mathbf{Z}_m$ 中，求一个元素 a 的平方根，其中 $m = pq$，p，q 是不同的奇素数．这可以利用定理 5 求出来．我们通过下面的例子说明这一方法．

例 1　在 $\mathbf{Z}_{91}$ 中，求 $\bar{1}$ 的平方根．

解　$\mathbf{Z}_{91} = \mathbf{Z}/(91)$，由于 $91 = 7\times 13$，且 7 与 13 互素，因此据本章 §1 的命题 2，得

$$(91) = (7)(13) = (7)\cap(13).$$

于是据定理 5，得

$$\mathbf{Z}/(91) \cong \mathbf{Z}/(7) \oplus \mathbf{Z}/(13), \tag{26}$$

其中同构映射为

$$\psi: a + (91) \longmapsto (a + (7), a + (13)). \tag{27}$$

于是

$$\begin{aligned}
&(a + (91))^2 = 1 + (91)\\
\Longleftrightarrow\ &(a + (7), a + (13))^2 = (1 + (7), 1 + (13))\\
\Longleftrightarrow\ &(a + (7))^2 = 1 + (7)\ \text{且}\ (a + (13))^2 = 1 + (13).
\end{aligned}$$

由于 $\mathbf{Z}/(7)$，$\mathbf{Z}/(13)$ 都是域，而任一域 F 上的一元多项式环 $F[x]$ 中，n 次多项式 $f(x)$ 在 F 中至多有 n 个根（重根按重数计算），因此 x^2-1 在 $\mathbf{Z}/(7)$，$\mathbf{Z}/(13)$ 中分别至多有两个根．显然 $1+(7)$，$-1+(7)$ 是 $1+(7)$ 的两个不同的平方根；$1+(13)$，$-1+(13)$ 是 $1+(13)$ 的两个不同的平方根．因此

$$\begin{aligned}
&(a + (91))^2 = 1 + (91)\\
\Longleftrightarrow\ &a + (7) = \pm 1 + (7)\ \text{且}\ a + (13) = \pm 1 + (13)\\
\Longleftrightarrow\ &\begin{cases} a \equiv 1 \pmod 7, \\ a \equiv 1 \pmod{13}; \end{cases}\ \text{或}\ \begin{cases} a \equiv 1 \pmod 7, \\ a \equiv -1 \pmod{13}; \end{cases}\\
&\text{或}\ \begin{cases} a \equiv -1 \pmod 7, \\ a \equiv 1 \pmod{13}; \end{cases}\ \text{或}\ \begin{cases} a \equiv -1 \pmod 7, \\ a \equiv -1 \pmod{13}. \end{cases}
\end{aligned}$$

先解下列两个简单的同余方程组：

$$\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv 0 \pmod{13}. \end{cases} \longrightarrow x = e_1 = 78 + 91k, k \in \mathbf{Z};$$

$$\begin{cases} x \equiv 0 \pmod 7, \\ x \equiv 1 \pmod{13}. \end{cases} \longrightarrow x = e_2 = 14 + 91k, k \in \mathbf{Z}.$$

从而据(24)和(25)式得出同余方程组

$$\begin{cases} a \equiv 1 \pmod 7, \\ a \equiv 1 \pmod{13}. \end{cases}$$

的解为

$$a = 1 \times 78 + 1 \times 14 + 91k = 1 + 91l, \quad l \in \mathbf{Z}.$$

类似地，可得出上面的第二、三、四个同余方程组的解依次为

$$a = 1 \times 78 + (-1) \times 14 + 91k = 64 + 91k, \ k \in \mathbf{Z};$$

$$a = (-1) \times 78 + 1 \times 14 + 91k = 27 + 91l, \ l \in \mathbf{Z};$$

$$a = (-1) \times 78 + (-1) \times 14 + 91k = -1 + 91l, \ l \in \mathbf{Z}.$$

因此在 $\mathbf{Z}/(91)$ 中，$\bar{1}$ 的平方根恰好有 4 个：

$$\bar{1}, \overline{64}, \overline{27}, \overline{-1},$$

其中$\overline{64} = -\overline{27}$.

推论 7　设 R 是一个有单位元的环，它的理想 $I_1, I_2, \cdots, I_s$ 两两互素，并且 $I_1 \cap I_2 \cap \cdots \cap I_s = (0)$，则

$$R \cong R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s. \qquad \square$$

习题 2.2

1. 设

$$R = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbf{C} \right\},$$

证明环 R 与四元数体 $\mathbf{H}$ 同构.

2. 设 σ 是环 R 到到 R' 的一个满同态. 证明:

(1) 如果 I 是 R 的一个理想,则 $\sigma(I)$ 是 R' 的理想;

(2) 如果 I' 是 R' 的一个理想,则 $\sigma^{-1}(I')$ 是 R 的理想,且 $\mathrm{Ker}\sigma \subseteq \sigma^{-1}(I')$.

3. 韩信点兵问题:"有一队士兵,三三数余 2,五五数余一,七七数余四. 问:这队士兵有多少人?"

4. 在 $\mathbf{Z}/(35)$ 中,分别求 $\overline{1}$ 的平方根和 $\overline{4}$ 的平方根.

5. 在 $\mathbf{Z}/(35)$ 中,$\overline{2}$ 的平方根存在吗?$\overline{3}$ 的平方根存在吗?

*6. 设正整数 $n = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$,其中 $p_1,p_2,\cdots,p_s$ 是两两不同的素数,$r_i > 0$,$i = 1,2,\cdots,s$. 证明:

$$\mathbf{Z}/(n) \cong \mathbf{Z}/(p_1^{r_1}) \oplus \mathbf{Z}/(p_2^{r_2}) \oplus \cdots \oplus \mathbf{Z}/(p_s^{r_s}).$$

§3　素理想和极大理想,有限域的构造

在整数环 $\mathbf{Z}$ 中,素数起着基本建筑块的作用. 素数的特征是:

$$\text{大于 1 的整数 } p \text{ 是素数}$$
$$\Longleftrightarrow \text{从 } p \mid ab \text{ 可以推出 } p \mid a \text{ 或 } p \mid b.$$

(关于充分性成立的理由:用反证法,假如 $p = p_1p_2$,其中 $p_1 > 1$,$p_2 > 1$,则 $p \mid p_1p_2$. 由所设得 $p \mid p_1$ 或 $p \mid p_2$,矛盾.)

用理想的语言,上述结论可以写成

$$\text{大于 1 的整数 } p \text{ 是素数}$$
$$\Longleftrightarrow \text{从 } ab \in (p) \text{ 可以推出 } a \in (p) \text{ 或 } b \in (p).$$

类似地,在域 F 上的一元多项式环 $F[x]$ 中,不可约多项式起着基本建筑块的作用,不可约多项式的特征是:

$$\text{次数大于 0 的多项式 } p(x) \text{ 是不可约多项式}$$
$$\Longleftrightarrow \text{从 } p(x) \mid f(x)g(x) \text{ 可以推出}$$
$$p(x) \mid f(x) \text{ 或 } p(x) \mid g(x)$$

$$\Longleftrightarrow 从\ f(x)g(x) \in (p(x))\ 可以推出$$
$$f(x) \in (p(x))\ 或\ g(x) \in (p(x)).$$

由上述受到启发，我们抽象出下述概念：

定义 1　设 R 是一个有单位元 $1(\neq 0)$ 的交换环，P 是 R 的一个理想，且 $P \neq R$，如果从 $ab \in P$ 可以推出 $a \in P$ 或 $b \in P$，则 P 称为 R 的一个**素理想**(prime ideal).

从上面的分析知道，在整数环 $\mathbf{Z}$ 中，

$$p\ 是素数$$
$$\Longleftrightarrow (p)\ 是\ \mathbf{Z}\ 的素理想.$$

在域 F 上的一元多项式环 $F[x]$ 中，

$$p(x)\ 是不可约多项式$$
$$\Longleftrightarrow (p(x))\ 是\ F[x]\ 的素理想.$$

从定义 1 立即得到，设 R 是一个有单位元 $1(\neq 0)$ 的交换环，则

$$(0)\ 是\ R\ 的一个素理想$$
$$\Longleftrightarrow R\ 是整环.$$

定义 2　设 R 是一个有单位元 $1(\neq 0)$ 的交换环，则 R 的所有素理想组成的集合称为 R 的**谱**(spectrum)，记作 $\mathrm{Spec}R$.

为了求整数环 $\mathbf{Z}$ 的谱，我们先证一个结论：

命题 1　环 $\mathbf{Z}$ 的每一个理想都是由一个非负整数生成的主理想.

证明　设 I 是 $\mathbf{Z}$ 的一个理想，如果 $I=(0)$，则 I 是主理想. 下面设 $I \neq (0)$. 于是存在 $a \in I$ 且 $a \neq 0$. 如果 a 是负整数，则 $-a=(-1)a \in I$. 因此 I 必含有正整数. 在 I 里的正整数中取一个最小的数，设为 m. 我们来证 $I=(m)$. 任取 $b \in I$，作带余除法：

$$b = qm + r,\quad 0 \leqslant r < m.$$

于是 $r=b-qm \in I$，假如 $r \neq 0$，则与 m 的取法矛盾，因此 $r=0$，即 $b=qm \in (m)$. 因此 $I \subseteq (m)$. 从而 $I=(m)$. □

由命题 1 和前面的结论立即得到整数环 $\mathbf{Z}$ 的谱为

$$\mathrm{Spec}\mathbf{Z} = \{(0)\} \cup \{(p) \mid p \text{ 为素数}\}. \tag{1}$$

类似于命题 1 的证明方法,可以证明下述的命题 2:

命题 2 域 F 上一元多项式环 $F[x]$ 的每一个理想都是主理想.其中非(0) 的主理想可以由首项系数为 1 的多项式生成.

如果域 F 上每一个一元多项式在 F 中都有根,则 F 称为一个**代数封闭域**(algebraically closed field).显然如果 F 是一个代数封闭域,则 $F[x]$ 中的每一个不可约多项式都是一次多项式,于是由命题 2 和前面的结论可得出:

如果 F 是一个代数封闭域,则环 $F[x]$ 的谱为

$$\mathrm{Spec}F[x] = \{(0)\} \cup \{(x-a) \mid a \in F\}. \tag{2}$$

定理 3 设 R 是有单位元 $1(\neq 0)$ 的交换环,则 R 的理想 P 为素理想当且仅当商环 R/P 为一个整环.

证明 显然商环 R/P 是有单位元 $1+P$ 的交换环.

R 的理想 P 为素理想.

$\Longleftrightarrow P \neq R$ 且从 $ab \in P$ 可推出 $a \in P$ 或 $b \in P$

$\Longleftrightarrow 1 \overline{\in} P$ 且从 $ab + P = P$ 可推出 $a + P = P$ 或 $b + P = P$

$\Longleftrightarrow 1 + P \neq P$ 且从 $(a+P)(b+P) = P$ 可推出 $a + P = P$ 或 $b + P = P$

$\Longleftrightarrow 1 + P \neq P$ 且 R/I 没有非平凡的零因子

$\Longleftrightarrow R/I$ 为一个整环. □

定理 4 设 R 和 R' 都是有单位元的交换环,且 $1 \neq 0, 1' \neq 0$.如果环 R 到 R' 有一个满同态 σ,则

(1) R' 的所有理想组成的集合 S' 与 R 的包含 $\mathrm{Ker}\sigma$ 的所有理想组成的集合 S 之间有一个一一对应;

(2) 对于 R 的包含 $\mathrm{Ker}\sigma$ 的理想 I,有

$$R/I \cong R'/\sigma(I);$$

(3) $\mathrm{Spec}R'$ 与 R 的包含 $\mathrm{Ker}\sigma$ 的所有素理想组成的集合 S_1 之间

有一个一一对应.

证明 容易验证，如果 I' 是 R' 的一个理想，则 $\sigma^{-1}(I')$ 是 R 的一个理想，且 $\sigma^{-1}(I') \supseteq \mathrm{Ker}\sigma$. 如果 I 是 R 的一个理想，则 $\sigma(I)$ 是 R' 的一个理想.

(1) 令 $\psi: S' \longrightarrow S$

$$I' \longmapsto \sigma^{-1}(I').$$

显然 ψ 是 S' 到 S 的一个映射.

可以证明 ψ 是满射，为此任取 $I \in S$，则 $\sigma(I) \in S'$. 想证 $\psi(\sigma(I)) = I$. 由于 $\psi(\sigma(I)) = \sigma^{-1}(\sigma(I))$，因此只要证

$$\sigma^{-1}(\sigma(I)) = I.$$

任取 $b \in \sigma^{-1}(\sigma(I))$，则 $\sigma(b) \in \sigma(I)$. 于是存在 $c \in I$，使得 $\sigma(c) = \sigma(b)$. 从而 $\sigma(b-c) = 0$. 因此 $b - c \in \mathrm{Ker}\sigma \subseteq I$. 于是 $b \in I$. 因此 $\sigma^{-1}(\sigma(I)) \subseteq I$. 反之，任取 $d \in I$，则 $\sigma(d) \in \sigma(I)$，从而 $d \in \sigma^{-1}(\sigma(I))$. 因此 $I \subseteq \sigma^{-1}(\sigma(I))$. 从而 $\sigma^{-1}(\sigma(I)) = I$.

可以证明 ψ 是单射. 设 I', J' 是 R' 的两个理想，如果 $\psi(I') = \psi(J')$，即 $\sigma^{-1}(I') = \sigma^{-1}(J')$，则对于任意 $a' \in I'$，存在 $a \in \sigma^{-1}(I')$，使得 $\sigma(a) = a'$. 由于 $\sigma^{-1}(I') = \sigma^{-1}(J')$，因此 $a \in \sigma^{-1}(J')$，从而 $\sigma(a) \in J'$. 即 $a' \in J'$. 因此 $I' \subseteq J'$. 同理 $J' \subseteq I'$，从而 $I' = J'$. 这表明 ψ 是单射.

(2) 设 I 是 R 的包含 $\mathrm{Ker}\sigma$ 的一个理想，由于 σ 是环 R 到 R' 的一个满同态，因此

$$R/\mathrm{Ker}\sigma \cong R'. \tag{3}$$

把 σ 限制到 I 上，则 $\sigma|I$ 是环 I 到 $\sigma(I)$ 的一个满同态. 由于 $\mathrm{Ker}\sigma \subseteq I$，因此 $\mathrm{Ker}(\sigma|I) = \mathrm{Ker}\sigma$. 从而有

$$I/\mathrm{Ker}\sigma \cong \sigma(I). \tag{4}$$

据第二环同构定理，得

$$R/I \cong (R/\mathrm{Ker}\sigma)/(I/\mathrm{Ker}\sigma). \tag{5}$$

从(3)、(4)、(5)式得

$$R/I \cong R'/\sigma(I). \tag{6}$$

(3) 设 P' 是 R' 的一个理想. 记 $P = \sigma^{-1}(P')$. 则 $P \supseteq \mathrm{Ker}\sigma$, 且有

$$\psi(\sigma(P)) = \sigma^{-1}(\sigma(P)) = P.$$

又有 $\psi(P') = \sigma^{-1}(P') = P$. 由于 ψ 是单射, 因此

$$\sigma(P) = P'.$$

从定理 3 和(6)式得

$$\begin{aligned} & P' \text{ 为 } R' \text{ 的一个素理想} \\ \Longleftrightarrow\ & R'/P' \text{ 为整环} \\ \Longleftrightarrow\ & R/P \text{ 为整环} \\ \Longleftrightarrow\ & P \text{ 为 } R \text{ 的一个素理想.} \end{aligned}$$

因此 ψ 在 $\mathrm{Spec}R'$ 上的限制是 $\mathrm{Spec}R'$ 到 R 的包含 $\mathrm{Ker}\sigma$ 的所有素理想组成的集合的一个双射. □

推论 5　设 R 是一个环, I 是 R 的一个理想, 则

(1) 商环 R/I 的所有理想组成的集合 S' 与 R 的包含 I 的所有理想组成的集合 S 之间有一个一一对应;

(2) 商环 R/I 的所有理想组成的集合 S' 为

$$S' = \{K/I \mid K \text{ 是 } R \text{ 的理想, 且 } K \supseteq I\}. \tag{7}$$

证明　环 R 到商环 R/I 有一个自然满同态 π, 且 $\mathrm{Ker}\pi = I$.

(1) 据定理 4 知道, $\psi: K/I \mapsto \pi^{-1}(K/I)$ 是 S' 到 S 的一个双射.

(2) 任取 $K/I \in S'$, 则 $\psi(K/I) = \pi^{-1}(K/I) \in S$. 记 $\widetilde{K} = \pi^{-1}(K/I)$, 则 $\widetilde{K} \in S$. 从而有

$$\psi(\pi(\widetilde{K})) = \pi^{-1}(\pi(\widetilde{K})) = \widetilde{K}.$$

即 $\psi(\widetilde{K}/I) = \widetilde{K}$. 又由上述知 $\psi(K/I) = \pi^{-1}(K/I) = \widetilde{K}$. 由于 ψ 是单射, 因此 $\widetilde{K}/I = K/I$. 从而 $K = \widetilde{K} \in S$. 这表明 K/I 属于(7)式右边的集合. 从而 S' 包含于(7)式右边的集合.

反之, 设 K 是 R 的理想, 且 $K \supseteq I$, 由于 $\pi(K)$ 是 R/I 的理想,

因此 $K/I=\pi(K)\in S'$,从而(7)式右边的集合包含于 S'.

综上所述得出(7)式成立,即商环 R/I 的所有理想组成的集合为

$$\{K/I \mid K \text{ 是 } R \text{ 的理想,且 } K\supseteq I\}.$$ ∎

设 R 是有单位元 $1(\neq 0)$ 的交换环,从定理 3 知道,R 的素理想 P 使得商环 R/P 为整环.自然要问:R 的什么样的理想 I 使得 R/I 为一个域?从习题 2.1 的第 5 题和第 6 题,以及推论 5 得出:

R/I 为一个域

$\Longleftrightarrow R/I$ 没有非平凡的理想,且 $1+I\neq I$

$\Longleftrightarrow R/I$ 的理想只有(0)(即 I/I)和 R/I,且 $I\neq R$

$\Longleftrightarrow R$ 中包含 I 的理想只有 I 和 R,且 $I\neq R$.

由此引出下述概念.

定义 3 设 R 是一个环,M 是 R 的一个理想,并且 $M\neq R$.如果 R 中包含 M 的理想只有 M 和 R,则 M 称为环 R 的一个**极大理想**(maximal ideal).

从上面的分析立即得出下述结论:

定理 6 设 R 是一个有单位元 $1(\neq 0)$ 的交换环,则 R 的理想 M 为极大理想当且仅当商环 R/M 为一个域. ∎

例如,在域 F 上的一元多项式环 $F[x]$ 中,如果 $p(x)$ 是不可约多项式,则 $(p(x))$ 是 $F[x]$ 的一个极大理想.理由如下:

设 $F[x]$ 的一个理想 $J\supseteq(p(x))$.由命题 2 得,$J=(f(x))$.于是 $(f(x))\supseteq(p(x))$.从而 $p(x)\in(f(x))$.因此 $f(x)\mid p(x)$.由此推出,$f(x)=c\in F^*$ 或 $f(x)=cp(x)$,其中 $c\in F^*$,从而 $J=(c)=F[x]$ 或 $J=(cp(x))=(p(x))$.因此 $(p(x))$ 是 $F[x]$ 的一个极大理想.

反之,如果 M 是 $F[x]$ 的一个极大理想,则 M 是由一个不可约多项式生成的理想.(设 $M=(g(x))$,假如 $g(x)$ 可约,则 $g(x)=g_1(x)g_2(x)$,$\deg g_i(x)<\deg g(x)$,$i=1,2$.于是 $(g_1(x))\supsetneqq$

$(g(x))$，且$(g_1(x)) \neq F[x]$. 这与 M 是极大理想矛盾.)

类似地，在 $\mathbf{Z}$ 中，M 是 $\mathbf{Z}$ 的一个极大理想当且仅当 M 是由一个素数生成的理想.

据定义 3，如果 F 是一个域，则(0) 是 F 的极大理想；反之，一个有单位元 $1(\neq 0)$ 的交换环 R，如果(0) 是 R 的极大理想，则 R 是一个域.

由于域一定是整环，但是整环不一定是域，因此在有单位元 $1(\neq 0)$ 的交换环 R 中，极大理想 M 一定是素理想，但是素理想 P 不一定是极大理想.

例如，在整系数一元多项式环 $\mathbf{Z}[x]$ 中，考虑(x)，商环 $\mathbf{Z}[x]/(x)$ 的每一个元素形如

$$a_0 + a_1x + \cdots + a_nx^n + (x) = a_0 + (x),$$

令 $\psi: a_0 \mapsto a_0 + (x)$. 显然 ψ 是环 $\mathbf{Z}$ 到 $\mathbf{Z}[x]/(x)$ 的一个同构映射. 因此 $\mathbf{Z} \cong \mathbf{Z}[x]/(x)$. 由于 $\mathbf{Z}$ 是整环，但不是域，因此 $\mathbf{Z}[x]/(x)$ 是整环，但不是域. 从而(x) 是 $\mathbf{Z}[x]$ 的一个素理想，但它不是极大理想.

设 R' 和 R 都是有单位元的交换环，且 $1' \neq 0'$，$1 \neq 0$. 如果环 R 到 R' 有一个单同态 σ，则 R 可以嵌入到 R'，此时称 R' 可看成是 R 的一个**扩环**(extension ring)，并且可以把 a 与 $\sigma(a)$ 等同. 特别地，如果 R' 有一个子环 R_1 与 R' 有相同的单位元，则称 R' 是 R_1 的一个**扩环**.

利用定理 6 可以从小的有限域出发构造大的有限域.

定理 7 设 F_q 是含 q 个元素的有限域，其中 $q = p^r$，p 为素数. 如果 $m(x) = a_0 + a_1x + \cdots + a_nx^n$ 是 $F_q[x]$ 的 n 次不可约多项式，则 $F_q[x]/(m(x))$ 是含 q^n 个元素的有限域，并且它的每一个元素可以唯一地表示成

$$c_0 + c_1u + \cdots + c_{n-1}u^{n-1}, \tag{8}$$

其中 $c_i \in F_q$，$0 \leqslant i < n$，$u = x + (m(x))$，u 满足

$$a_0 + a_1u + \cdots + a_nu^n = 0. \tag{9}$$

证明 由于 $m(x)$ 是 $F_q[x]$ 的不可约多项式,因此 $(m(x))$ 是 $F_q[x]$ 的一个极大理想. 据定理 6 得,$F_q[x]/(m(x))$ 是一个域. $F_q[x]/(m(x))$ 中每一个元素形如 $f(x)+(m(x))$. 作带余除法:

$$f(x)=h(x)m(x)+r(x),\deg r(x)<\deg m(x).$$

于是可以设 $r(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$. 从而

$$f(x)+(m(x))=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x)), \tag{10}$$

并且每一个陪集 $f(x)+(m(x))$ 表示成(10)式的表示方式唯一(假如 $f(x)+(m(x))$ 有两种表示方式:$r(x)+(m(x))$ 和 $r_1(x)+(m(x))$,其中 $\deg r(x)<n,\deg r_1(x)<n$,则 $r(x)-r_1(x)\in(m(x))$. 从而 $r(x)-r_1(x)=0$. 即 $r(x)=r_1(x)$). 由于 $c_i\in F_q$, $0\leqslant i<n$,因此每个 c_i 有 q 种选取方式,从而 $|F_q(x)/(m(x))|=q^n$.

令 $u=x+(m(x))$,由于 F_q 到 $F_q(x)/(m(x))$ 有一个单同态 $\sigma:a\to a+(m(x))$,因此可以把 a 与 $a+(m(x))$ 等同. 从而有

$$\begin{aligned}
&c_0+c_1x+\cdots+c_{n-1}x^{n-1}+(m(x))\\
&=[c_0+(m(x))]+[c_1+(m(x))][x+(m(x))]+\cdots\\
&\quad+[c_{n-1}+(m(x))][x+(m(x))]^{n-1}\\
&=c_0+c_1u+\cdots+c_{n-1}u^{n-1}.
\end{aligned} \tag{11}$$

因此

$$\begin{aligned}
F_q[x]/(m(x))=\{&c_0+c_1u+\cdots+c_{n-1}u^{n-1}\mid\\
&c_i\in F_q,0\leqslant i<n\}.
\end{aligned} \tag{12}$$

类似于(11)式的推导过程可得出

$$\begin{aligned}
a_0+a_1u+\cdots+a_nu^n&=a_0+a_1x+\cdots+a_nx^n+(m(x))\\
&=(m(x)).
\end{aligned}$$

因此在商环 $F_q[x]/(m(x))$ 中,$a_0+a_1u+\cdots+a_nu^n=0$. □

注:有限域 F 的元素个数 q 一定是一个素数 p 的方幂,其中 p 是

域 F 的特征．证明可参看丘维声编著的《高等代数(下册)》(高教社 1996 年出版)第 206－208 页．

例 1　构造含 125 个元素的有限域．

解　$125=5^3$．在 $\mathbf{Z}_5[x]$ 中找一个 3 次不可约多项式．令 $m(x)=x^3+x+1$．直接计算知道，$\mathbf{Z}_5$ 中，0，1，2，3，4 都不是 $m(x)$ 的根，又由于 $\deg m(x)=3$，因此 $m(x)$ 是不可约多项式．从而 $\mathbf{Z}_5[x]/(x^3+x+1)$ 是含 5^3 个元素的有限域．令 $u=x+(x^3+x+1)$，则

$$\mathbf{Z}_5[x]/(x^3+x+1)=\{c_0+c_1u+c_2u^2\mid c_i\in\mathbf{Z}_5,i=0,1,2\},$$

其中 u 满足 $u^3+u+1=0$，即 $u^3=4u+4$．

定理 8　*在有单位元 $1(\neq 0)$ 的环 R 中必存在极大理想．*

证明　令 $S=\{I\mid I$ 是 R 的理想，且 $1\overline{\in}I\}$．显然 $(0)\in S$，因此 S 为非空集．S 按照集合的包含关系成为一个偏序集．即，S 有一个二元关系 $\subseteq$，它具有反身性，反对称性(若 $I_1\subseteq I_2$ 且 $I_2\subseteq I_1$，则 $I_1=I_2$)，和传递性．

任取 S 的一条链 $T=\{I_\alpha\in S\mid\alpha\in J\}$，其中 J 是指标集．即对于 T 中任意两个元素 I_α 与 I_β，必有 $I_\alpha\subseteq I_\beta$ 或者 $I_\beta\subseteq I_\alpha$．令 $A=\bigcup\limits_{\alpha\in J}I_\alpha$．容易证明 A 是 R 的一个理想，且 $1\overline{\in}A$，因此 $A\in S$．由于 $I_\alpha\subseteq A$，$\forall\alpha\in J$，因此 A 是 T 的一个上界．根据 Zorn 引理(如果一个偏序集 S 的每一条链都有上界，则 S 有一个极大元素)得，S 有一个极大元素 M．于是 M 是 R 的一个理想，且 $1\overline{\in}M$，从而 $M\neq R$．据极大元素的定义，任取 $H\in S$，从 $M\subseteq H$ 可推出 $M=H$．因此 M 是 R 的一个极大理想．　□

习题 2.3

1．证明本节命题 2：域 F 上一元多项式环 $F[x]$ 的每一个理想都

是主理想，其中非(0)的主理想可以由首项系数为1的多项式生成．

2．设 R 是有单位元 $1(\neq 0)$ 的交换环，R_1 是 R 的一个子环，并且 R_1 与 R 有相同的单位元．设 P 是 R 的一个素理想，证明 $P\cap R_1$ 是 R_1 的一个素理想．

*3．求 $\mathrm{Spec}\mathbf{Z}/(30)$．

4．设 F 是一个域，证明：如果 $p(x)$ 是 $F[x]$ 的不可约多项式，则 $F[x]/(p(x))$ 是一个域．

5．设 F 是一个域，证明：如果 $f(x)$ 是 $F[x]$ 的可约多项式，则 $F[x]/(f(x))$ 有非平凡的零因子．

6．构造含4个元素的有限域，写出它的加法运算表和乘法运算表．

7．构造含9个元素的有限域．

8．构造含8个元素的有限域．

*9．设 $R=2\mathbf{Z}$，证明(4)是 R 的一个极大理想，但是 $R/(4)$ 不是域．

*10．设 R 是有单位元 $e(\neq 0)$ 的环，令 $\mathbf{Z}e \xlongequal{\text{def}} \{ne \mid n\in\mathbf{Z}\}$．

(1) 证明 $\mathbf{Z}e$ 是 R 的一个子环，且 $\mathbf{Z}/(m)\cong\mathbf{Z}e$，其中 m 是某一个非负整数；我们把 m 叫做环 R 的**特征**．

(2) 如果 R 是整环，则 R 的特征为0或者为一个素数．

*11．设 R 是一个有单位元 $1(\neq 0)$ 的交换环，证明 R 的所有素理想的交等于 R 的幂零根 $\mathrm{rad}(0)$．

*12．设正整数 $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$，其中 $p_1,p_2,\cdots,p_s$ 是两两不同的素数，$e_i>0,1\leqslant i\leqslant s$．证明 $\mathbf{Z}/(n)$ 的幂零根为

$$(p_1p_2\cdots p_s)/(n).$$

§4　代数数域和 Galois 环的构造

在上一节我们介绍了从 q 元有限域 F_q 出发，构造 q^n 元有限域的

方法，首先在 $F_q[x]$ 中找一个 n 次不可约多项式 $m(x)$；然后作商环 $F_q[x]/(m(x))$，它就是 q^n 元有限域，它的每一个元素可唯一地表示成

$$c_0 + c_1 u + \cdots + c_{n-1} u^{n-1}, \quad c_i \in F_q, \quad 0 \leqslant i < n, \tag{1}$$

其中 $u = x + (m(x))$，它满足 $m(u) = 0$.

这种方法也适用于任意一个域 F.

例如，设 F 为实数域 $\mathbf{R}$，在 $\mathbf{R}[x]$ 中取一个 2 次不可约多项式 $m(x) = x^2 + 1$；作商环 $\mathbf{R}[x]/(x^2 + 1)$，则它是域，并且

$$\mathbf{R}[x]/(x^2 + 1) = \{a + bu \mid a, b \in \mathbf{R}\}. \tag{2}$$

其中 $u = x + (x^2 + 1)$，它满足 $u^2 + 1 = 0$，即 $u^2 = -1$. 令

$$\sigma: \mathbf{R}[x]/(x^2 + 1) \longrightarrow \mathbf{C}$$
$$a + bu \longmapsto a + bi.$$

容易验证 σ 是一个环同构，因此域 $\mathbf{R}[x]/(x^2 + 1)$ 与复数域 $\mathbf{C}$ 同构. 顺便看到，虽然在 $\mathbf{R}$ 中不存在 $\sqrt{-1}$，但是在域 $\mathbf{R}[x]/(x^2 + 1)$ 中，有 $u^2 = -1$，从而 $u = \sqrt{-1}$（这里我们把 -1 与 $-1 + (x^2 + 1)$ 等同）.

$\mathbf{R}[x]$ 中的不可约多次式只有 1 次多项式和判别式小于 0 的 2 次多项式. 不难看出，在 $\mathbf{R}[x]$ 中取任意一个 2 次不可约多项式 $p(x)$，得到的域 $\mathbf{R}[x]/(p(x))$ 都与复数域 $\mathbf{C}$ 同构. 于是我们转而考虑从有理数域 $\mathbf{Q}$ 出发. 因为 $\mathbf{Q}[x]$ 中有任意次数的不可约多项式，所以可以从 $\mathbf{Q}$ 出发构造出一大批域.

在 $\mathbf{Q}[x]$ 中取一个 n 次不可约多项式 $m(x)$，便得到一个域 $\mathbf{Q}[x]/(m(x))$. 为了看出它同构于什么样的域，我们现在介绍从 $\mathbf{Q}$ 出发构造域的另一种方法.

定义 1　设 R 是有单位元 $1(\neq 0)$ 的交换环，R' 是 R 的一个扩环，且 R' 是交换环. 任意取定 $u \in R'$，我们把 R' 中包含 R 和 u 的所有子环的交称为 **u 在 R 上生成的子环**，或 **R 添加 u 得到的子环**，记作 $R[u]$.

容易证明

$$R[u]=\{a_0+a_1u+\cdots+a_nu^n\mid a_i\in R,0\leqslant i\leqslant n,n\in\mathbf{N}\},\tag{3}$$

其中 $a_0+a_1u+\cdots+a_nu^n$ 称为 u **在 R 上的一个多项式**.

现在取 $R=\mathbf{Q},R'=\mathbf{C}$,任意取定一个复数 t,令

$$\sigma_t:\mathbf{Q}[x]\longrightarrow\mathbf{Q}[t]$$

$$f(x)=\sum_{i=0}^{n}a_ix^i\ \mapsto\sum_{i=0}^{n}a_it^i\xlongequal{\text{def}}f(t).\tag{4}$$

容易验证 σ_t 是环 $\mathbf{Q}[x]$ 到 $\mathbf{Q}[t]$ 的一个满同态,从而

$$\mathbf{Q}[x]/\mathrm{Ker}\sigma_t\cong\mathbf{Q}[t],\tag{5}$$

$$f(x)\in\mathrm{Ker}\sigma_t\Longleftrightarrow f(t)=0$$

$$\Longleftrightarrow f(x)\text{ 以 }t\text{ 为一个复根}.$$

于是

$$\mathrm{Ker}\sigma_t=\{f(x)\in\mathbf{Q}[x]\mid f(x)\text{ 以 }t\text{ 为一个复根}\}.$$

这表明 $\mathbf{Q}[x]$ 中以 t 为一个复根的所有多项式组成的集合是一个理想. 由于 $\mathbf{Q}[x]$ 的每一个理想是主理想,因此 $\mathrm{Ker}\sigma_t=(0)$ 或 $\mathrm{Ker}=(p(x))$. 在后一情形,可以取到 $p(x)$ 是首项系数为 1 的多项式,且 $p(x)$ 是以 t 为一个复根的所有非零多项式中次数最低的多项式,称 $p(x)$ 是 t 在 $\mathbf{Q}$ 上的**极小多项式**(minimal polynomial). 显然,$p(x)$ 一定是 $\mathbf{Q}[x]$ 中的不可约多项式. 从而 $\mathbf{Q}[x]/(p(x))$ 是一个域. 据(5)式得,$\mathbf{Q}[t]$ 是一个域. 设

$$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,\quad a_i\in\mathbf{Q},0\leqslant i<n,$$

则从 $p(t)=0$ 得,$t^n=-a_{n-1}t^{n-1}-\cdots-a_1t-a_0$. 因此

$$\mathbf{Q}[t]=\{c_0+c_1t+\cdots+c_{n-1}t^{n-1}\mid c_i\in\mathbf{Q},0\leqslant i<n\}.$$

由于 $p(x)$ 不可约,因此 $\mathbf{Q}[t]$ 中每一个元素表示成 $c_0+c_1t+\cdots+c_{n-1}t^{n-1}$ 的表法唯一.

前面通过在 $\mathbf{Q}[x]$ 中先找一个不可约多项式 $m(x)$,然后作商

环 $\mathbf{Q}[x]/(m(x))$ 得到一个域.设 t 是 $m(x)$ 的一个复根,则 $\mathbf{Q}[x]$ 到 $\mathbf{Q}[t]$ 的满同态 σ_t 的核等于 $(m(x))$. 因此 $\mathbf{Q}[x]/(m(x)) \cong \mathbf{Q}[t]$. 这表明作商环 $\mathbf{Q}[x]/(m(x))$ 得到域的方法与 $\mathbf{Q}$ 添加 t 得到域 $\mathbf{Q}[t]$ 的方法在本质上是一致的.

定义 2 如果一个复数 t 是 $\mathbf{Q}[x]$ 中某个非零多项式的根,则 t 称为一个**代数数**(algebraic number);否则,t 称为一个**超越数**(transcendental number).

定义 3 如果一个复数 α 是某个首项系数为 1 的整系数多项式的根,则 α 称为一个**代数整数**(algebraic integer).

从前面的分析知道,如果 t 是一个代数数,则存在一个以 t 为根的次数最低的首项系数为 1 的多项式 $p(x)$,它一定是 $\mathbf{Q}[x]$ 中的不可约多项式,并且 $\mathbf{Q}[x]/(p(x)) \cong \mathbf{Q}[t]$. 于是 $\mathbf{Q}[t]$ 是一个域. 这表明有理数域 $\mathbf{Q}$ 添加一个代数数 t 得到的子环 $\mathbf{Q}[t]$ 是一个域,$\mathbf{Q}[t]$ 称为一个**代数数域**(algebraic number field),此时把 $\mathbf{Q}[t]$ 也记成 $\mathbf{Q}(t)$.

例如,$p(x) = x^2 + x + 1$ 是 $\mathbf{Q}[x]$ 中的不可约多项式,它的一对共轭虚根是 $\omega = \dfrac{-1+\sqrt{3}\mathrm{i}}{2}$,$\omega^2 = \dfrac{-1-\sqrt{3}\mathrm{i}}{2}$. 因此 ω 是一个代数数. 从而 $\mathbf{Q}[\omega]$ 是一个代数数域.

我们知道,复数域中,对于给定的正整数 n,所有 n 次单位根组成的集合对于乘法成为一个循环群 U_n. 这个循环群的一个生成元称为一个**本原 n 次单位根**(primitive nth root of unity). 例如 $\xi_n = \mathrm{e}^{\mathrm{i}\frac{2\pi}{n}}$ 是一个本原 n 次单位根. $\mathbf{Q}$ 添加一个本原 n 次单位根 ξ_n 得到的域 $Q[\xi_n]$ 称为第 n 个**分圆域**(cyclotomic field),也记成 $Q(\xi_n)$.

例如,$\omega = \dfrac{-1+\sqrt{3}\mathrm{i}}{2}$ 是 3 次单位根. 于是 $\mathbf{Q}[\omega]$(或写成 $\mathbf{Q}(\omega)$)是第 3 个分圆域.

现在我们把上面从小的域出发构造大的域的方法推广到有单位元 $1(\neq 0)$ 的交换环上,从小的环构造出一批大的环. 以下都假设 R

是有单位元 $1(\neq 0)$ 的交换环.

首先需要有环 R 上的一元多项式环 $R[x]$. 关于环 R 上一元多项式的定义与数域 K 上一元多项式的定义一样,这里就不写出了. 关于数域 K 上一元多项式的定义可参看丘维声编著的《高等代数(下册)》(高教社 1996 年出版)第 2 页. 环 R 上所有一元多项式组成的集合记作 $R[x]$. 在 $R[x]$ 中规定加法和乘法两种运算(与数域 K 上一元多项式环 $K[x]$ 中加法和乘法的定义一样),从而 $R[x]$ 成为有单位元 $1(\neq 0)$ 的交换环,称它为**环 R 上的一元多项式环**.

设 R' 是 R 的一个扩环,且 R' 是交换环. 任意取定 $t \in R'$,令

$$\sigma_t: R[x] \longrightarrow R[t]$$

$$f(x) = \sum_{i=0}^{n} a_i x^i \longmapsto \sum_{i=0}^{n} a_i t^i \stackrel{\text{def}}{=\!=} f(t). \tag{6}$$

容易验证 σ_t 是环 $R[x]$ 到 $R[t]$ 的一个满同态,并且

$$\sigma_t(x) = t, \quad \sigma_t(a) = a, \quad \forall\, a \in R; \tag{7}$$

从而

$$R[x]/\mathrm{Ker}\sigma_t \cong R[t], \tag{8}$$

容易看出 $\mathrm{Ker}\sigma_t \cap R = \{0\}$,并且

$$\mathrm{Ker}\sigma_t = \{f(x) \in R[x] \mid f(x) \text{ 以 } t \text{ 为一个根}\}.$$

如果 $\mathrm{Ker}\sigma_t = (0)$,则对每一个非零多项式 $f(x)$ 都有 $f(t) \neq 0$. 此时称 t 在 R 上是**超越的**(transcendental over R),或者称 t 是 R 上的**超越元**.

如果 $\mathrm{Ker}\,\sigma_t \neq (0)$,则在 $R[x]$ 中存在 $f(x) \neq 0$,使得 $f(t) = 0$,此时称 t 在 R 上是**代数的**(algebraic over R),或者称 t 是 R 上的**代数元**.

反之,给了 $R[x]$ 一个理想 I,且 $I \cap R = \{0\}$,则有 $R[x]$ 到 $R[x]/I$ 的自然满同态 π,且 $\mathrm{Ker}\pi = I$. π 在 R 上的限制 $\pi|R$ 为 $a \longmapsto a + I$. 由于 $I \cap R = \{0\}$,因此 $\pi|R$ 是单射. 从而 $\pi|R$ 是环 R 到

$R[x]/I$ 的单同态.于是可以把 $R[x]/I$ 看成是 R 的一个扩环,把 a 与 $a+I$ 等同.令 $u=x+I$,则

$$R[x]/I=\{a_0+a_1u+\cdots+a_nu^n \mid a_i\in R,0\leqslant i\leqslant n,n\in \mathbf{N}\}. \tag{9}$$

即 $R[x]/I=R[u]$.这样我们从环 R 出发构造出了环 $R[x]/I$.

现在取 $R=\mathbf{Z}_4$,在 $\mathbf{Z}_4[x]$ 中取一个多项式 $f(x)$:

$$f(x)=x^3+2x^2+x+3.$$

把 $f(x)$ 的每一项的系数模 2(即 $0\mapsto 0,1\mapsto 1,2\mapsto 0,3\mapsto 1$),使得到 $\mathbf{Z}_2[x]$ 中的一个多项式 $\bar{f}(x)=x^3+x+1$.容易看出,$\bar{f}(x)$ 是 $\mathbf{Z}_2[x]$ 中的不可约多项式,且首项系数为 1,此时我们称 $f(x)$ 在 $\mathbf{Z}_4[x]$ 中是**基本不可约的**(basic irreducible).作商环 $\mathbf{Z}_4[x]/(f(x))$,令 $u=x+(f(x))$,则在 $\mathbf{Z}_4[x]/(f(x))$ 中,有

$$f(u)=u^3+2u^2+u+3=0,$$

即 $u^3=2u^2+3u+1$.从而

$$\mathbf{Z}_4[x]/(f(x))=\{a_0+a_1u+a_2u^2 \mid a_i\in \mathbf{Z}_4,0\leqslant i\leqslant 2\}.$$

容易看出,$\mathbf{Z}_4[x]/(f(x))$ 中的每一个元素表成 $a_0+a_1u+a_2u^2$ 的表法唯一.于是 $|\mathbf{Z}_4[x]/(f(x))|=4^3$.$\mathbf{Z}_4[x]/(f(x))$ 可看成是 $\mathbf{Z}_4$ 的扩环.

一般地,设 p 是一个素数,r 是一个正整数.在环 $\mathbf{Z}_{p^r}$ 上的一元多项式环 $\mathbf{Z}_{p^r}[x]$ 中,一个首项系数为 1 的多项式 $f(x)$,如果把它的系数模 p 以后得到的多项式 $\bar{f}(x)$ 在 $\mathbf{Z}_p[x]$ 中不可约,则称 $f(x)$ 在 $\mathbf{Z}_{p^r}[x]$ 中是**基本不可约的**.

设 $f(x)$ 是 $\mathbf{Z}_{p^r}[x]$ 中的 m 次基本不可约多项式,则商环 $\mathbf{Z}_{p^r}[x]/(f(x))$ 是含有 $(p^r)^m$ 个元素的有限环,称它为一个 **Galois 环**,记作 $GR(p^r,m)$,或 $GR((p^r)^m)$,或 $R_{(p^r)^m}$,它可看成是 $\mathbf{Z}_{p^r}$ 的扩环.

上面求出的商环 $\mathbf{Z}_4[x]/(f(x))$ 就是一个 Galois 环,记作

$GR(4,3)$,或 $GR(4^3)$,或 R_{4^3}.

在 $\mathbf{Z}_{p^r}[x]$ 中找一个 m 次基本不可约多项式 $f(x)$ 的好处在于:此时一方面 $\mathbf{Z}_{p^r}[x]/(f(x))$ 是含 $(p^r)^m$ 个元素的有限环,另一方面 $\mathbf{Z}_p[x]/(\bar{f}(x))$ 是含 p^m 个元素的有限域,它们之间会有联系.

Galois 环在 1924 年被 Krull 研究过.在 1966 年和 1969 年分别由 Janusz 和 Raghavendran 独立地重新发现.自从 1994 年 Hammons 等人的文章"The $\mathbf{Z}_4$ - linearity of *Ker*dock, Preparata, Geothals, and related codes"发表以来,$\mathbf{Z}_4$ 上的线性码成了编码理论研究的一个热点,而 Galois 环 $GR(4^m)$ 起着重要作用.(参看 TOR HELLESETH and P. VIJAY KUMAR, Codes and Sequences over $\mathbf{Z}_4$—A Tutorial Overview, A. Pott et al. (eds.), Difference Sets, Sequences and their Correlation Properties, 1999, 195 - 225, 或者 Zhe - Xian Wan 著《Quaternary Codes》, Word Scientific, 1997.)

上面从环 R 出发,先作 R 上的一元多项式环 $R[x]$,然后作 $R[x]$ 对理想 I(I 满足 $I \cap R = (0)$)的商环 $R[x]/I$,从而构造出较大的环,这种方法可以作进一步的推广.

环 R 上的 n 元多项式环 $R[x_1, x_2, \cdots, x_n]$ 与数域 K 上的 n 元多项式环 $K[x_1, x_2, \cdots, x_n]$ 的形成过程一样.

设 R' 是 R 的一个扩环,且 R' 是交换环.$u_1, u_2, \cdots, u_n \in R'$.$R'$ 中包含 R 和 $u_1, u_2, \cdots, u_n$ 的所有子环的交称为**由 $u_1, u_2, \cdots, u_n$ 在 R 上生成的子环**,或称为 **R 添加 $u_1, u_2, \cdots, u_n$ 得到的子环**,记作 $R[u_1, u_2, \cdots, u_n]$,它的每个元素称为 $u_1, u_2, \cdots, u_n$ 在 R 上的多项式.

容易证明:

$$R[u_1, u_2, \cdots, u_n] = R[u_1][u_2]\cdots[u_n]. \tag{10}$$

类似于 $R[x]$ 到 $R[u]$ 有一个满同态 σ_u,存在 $R[x_1, x_2, \cdots, x_n]$ 到 $R[u_1, u_2, \cdots, u_n]$ 的一个满同态 $\eta: f(x_1, x_2, \cdots, x_n) \longmapsto f(u_1,$

$u_2, \cdots, u_n$),使得

$$\eta(x_i) = u_i,\ 1 \leqslant i \leqslant n; \quad \eta(a) = a,\ \forall a \in R; \tag{11}$$

从而

$$R[x_1, x_2, \cdots, x_n]/\mathrm{Ker}\,\eta \cong R[u_1, u_2, \cdots, u_n], \tag{12}$$

并且 $\mathrm{Ker}\,\eta \cap R = (0)$.

如果 $\mathrm{Ker}\,\eta = (0)$,则称 $u_1, u_2, \cdots, u_n$ 在 R 上是**代数无关的**(algebraically independent).

如果 $\mathrm{Ker}\,\eta \neq (0)$,则存在 R 上的非零 n 元多项式 $f(x_1, x_2, \cdots, x_n)$,使得 $f(u_1, u_2, \cdots, u_n) = 0$,此时称 $u_1, u_2, \cdots, u_n$ 在 R 上是**代数相关的**(algebraically dependent).

反之,给了 $R[x_1, x_2, \cdots, x_n]$ 的一个理想 I,且 $I \cap R = (0)$,则 $R[x_1, x_2, \cdots, x_n]$ 到商环 $R[x_1, x_2, \cdots, x_n]/I$ 有自然满同态 π,且 $\mathrm{Ker}\,\pi = I$. 由于 $I \cap R = (0)$,因此 $\pi|R$ 是 R 到 $R[x_1, x_2, \cdots, x_n]/I$ 的一个单同态. 从而 $R[x_1, x_2, \cdots, x_n]/I$ 可看成是 R 的一个扩环. 令 $u_i = x_i + I, i = 1, 2, \cdots, n$,则 $R[x_1, x_2, \cdots, x_n]I/$ 的每一个元素是 $u_1, u_2, \cdots, u_n$ 在 R 上的多项式. 从而 $R[x_1, x_2, \cdots, x_n]/I = R[u_1, u_2, \cdots, u_n]$.

我们在前面通过作 $R[x]$ 的商环 $R[x]/I$ 构造出一批环,为此我们需要了解 $R[x]$ 的一些性质:设 R 是有单位元 $1(\neq 0)$ 的交换环,

(1) 次数公式:

$$\deg(f(x) + g(x)) \leqslant \max(\deg f(x), \deg g(x)); \tag{13}$$

$$\deg(f(x)g(x)) \leqslant \deg f(x) + \deg g(x), \tag{14}$$

如果 $f(x)$ 或 $g(x)$ 的首项系数不是零因子,则(14)式的等号成立.

(2) 如果 $g(x)$ 的首项系数是可逆元,则带余除法成立.

(3) 整除的概念,因式、倍式的概念都有.

(4) 余数定理成立.

(5) 在 $R[x]$ 中，$x-a \mid f(x)$ 当且仅当 a 是 $f(x)$ 在 R 中的根.

如果 R 是整环，则 $R[x]$ 也是整环，$R[x_1,x_2,\cdots,x_n]$ 也是整环.

如果 R 是整环，则 $R[x]$ 中每一个 $n(\geqslant 0)$ 次多项式在 R 中至多有 n 个根(重根按重数计算).

习题 2.4

1. 证明：对于任意整数 m,n，复数 $m+n\mathrm{i}$ 是代数整数，称这种形式的代数整数为**高斯整数**.

2. 证明 $t=\sqrt{2}+\sqrt{3}$ 是一个代数数，求 t 的极小多项式.

3. 设 t 为 $f(x)=x^3-x+1$ 的一个复根. 在代数数域 $\mathbf{Q}[t]$ 中，求 $(5t^2+3t-1)(2t^2-2t+6)$ 和 $(3t^2-t+2)^{-1}$.

4. 在 $\mathbf{Z}_4[x]$ 中，设 $f(x)=x^3+2x^2+x+3$，$f(x)$ 是 $\mathbf{Z}_4[x]$ 中的基本不可约多项式，于是商环 $\mathbf{Z}_4[x]/(f(x))$ 是 Galois 环 $GR(4^3)$.

(1) $GR(4^3)$ 是整环吗?(x^3+2x^2+x+3) 是 $\mathbf{Z}_4[x]$ 的一个素理想吗?

(2) 令 $u=x+(f(x))$，求 u 在 $GR(4^3)$ 的单位群(即，$GR(4^3)$ 中所有可逆元素形成的乘法群)中的阶.

*3. 令 $\sigma:\ \mathbf{Z}_4[x]\longrightarrow \mathbf{Z}_2[x]$

$$g(x)\longmapsto \bar{g}(x),$$

其中 $\bar{g}(x)$ 是把 $g(x)$ 的系数模 2 以后得到的 $\mathbf{Z}_2[x]$ 中的多项式. 证明 σ 是一个满同态，并且 σ 诱导了 $\mathbf{Z}_4[x]/(f(x))$ 到 $\mathbf{Z}_2[x]/(\bar{f}(x))$ 的一个满同态：

$g(x)+(f(x))\longmapsto \bar{g}(x)+(\bar{f}(x))$，仍记为 σ.

*(4) 记 $\alpha=\sigma(u)$. 求 α 在有限域 $\mathbf{Z}_2[x]/(\bar{f}(x))$ 的乘法群中的阶.

*(5) 令 $\mathcal{T}=\{0\}\cup\{1,u,u^2,\cdots,u^{n-1}\}$，其中 n 是 u 的阶（在第(2)小题中已求出）．证明：对于 $\mathcal{T}$ 中任意两个元素 ν_1,ν_2，如果 $\sigma(\nu_1)=\sigma(\nu_2)$，则 $\nu_1=\nu_2$．

*(6) 设 $x_1,y_1,x_2,y_2\in\mathcal{T}$，证明：

$$x_1+2y_1=x_2+2y_2 \Longrightarrow x_1=x_2 \text{ 且 } y_1=y_2.$$

*(7) 证明：$GR(4^3)=\{x+2y \mid x,y\in\mathcal{T}\}$．（注：$GR(4^3)$ 中每个元素可唯一地表示成 $x+2y$，$x,y\in\mathcal{T}$，这称为 **2 - adic 表示**．）

*§5　分式域

在上一节我们从实数域 **R** 出发，构造了与复数域 **C** 同构的域 $\mathbf{R}[x]/(x^2+1)$；从有理数域 **Q** 出发，构造了一批代数数域 $\mathbf{Q}(t)$，其中 t 是代数数．但是有理数域 **Q** 本身，是从整数环出发构造的，**Z** 到 **Q** 有一个单的环同态 $\sigma: m\longmapsto \frac{m}{1}$，并且每一个有理数可以表示成 $\sigma(a)\sigma(b)^{-1}$，即 ab^{-1} 的形式，其中 $a,b\in\mathbf{Z}$，且 $b\neq 0$．此外，设 F 是一个域，任取 $f(x),g(x)\in F[x]$，且 $g(x)\neq 0$，则 $\frac{f(x)}{g(x)}$ 是一个分式．所有分式组成的集合对于熟知的分式的加法和乘法成为一个域，称它为域 F 上一元**有理函数域**(rational function field)，记作 $F(x)$．显然，从 $F[x]$ 到 $F(x)$ 有一个单的环同态 $\tau: f(x)\mapsto \frac{f(x)}{1}$，并且每一个分式都可以表示成 $\tau(f(x))\tau(g(x))^{-1}$，即 $f(x)g(x)^{-1}$ 的形式，其中 $f(x),g(x)\in F[x]$，且 $g(x)\neq 0$．从这两个例子我们引出下述概念：

定义 1　设 R 是一个整环，一个域 F 称为 R 的**分式域**(field of fractions)，如果 R 到 F 有一个单的环同态 σ，使得 F 中每个元素都可以表示成 $\sigma(a)\sigma(b)^{-1}$，即 ab^{-1} 的形式，其中 $a,b\in R$，且 $b\neq 0$．我

们常常把 ab^{-1} 写成 $\frac{a}{b}$.

每一个整环是否都存在分式域？回答是肯定的，下面我们给出构造的方法．

设 R 是一个整环，令

$$T = R \times R^* = \{(a,b) \mid a \in R, b \in R^*\}. \tag{1}$$

在集合 T 中规定一个二元关系 $\sim$ 如下：

$$(a,b) \sim (c,d) \overset{\text{def}}{\Longleftrightarrow} ad = bc. \tag{2}$$

容易证明 $\sim$ 是一个等价关系．把 (a,b) 确定的等价类记作 $\frac{a}{b}$，于是

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc. \tag{3}$$

用 F 表示商集 $T/\sim$．在 F 中规定

$$\frac{a}{b} + \frac{c}{d} \xlongequal{\text{def}} \frac{ad+bc}{bd}, \tag{4}$$

$$\frac{a}{b} \cdot \frac{c}{d} \xlongequal{\text{def}} \frac{ac}{bd}. \tag{5}$$

下面证明(4)式和(5)式与等价类的代表的选取无关．设

$$\frac{a}{b} = \frac{a'}{b'}, \quad \frac{c}{d} = \frac{c'}{d'}.$$

则

$$ab' = ba', \quad cd' = dc'.$$

由此得出

$$ab'dd' = ba'dd', \quad cd'bb' = dc'bb'.$$

从而 $$ab'dd' + cd'bb' = ba'dd' + dc'bb',$$

即 $$b'd'(ad + cb) = bd(a'd' + c'b').$$

因此 $$\frac{ad+cb}{bd} = \frac{a'd'+c'b'}{b'd'},$$

即 $$\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}.$$

因此(4)式给出的加法的定义是合理的.

类似地可证(5)式给出的乘法的定义是合理的.

容易验证,加法、乘法都适合交换律、结合律,并且适合乘法对于加法的分配律.

因为

$$\frac{0}{b}+\frac{c}{d}=\frac{0d+bc}{bd}=\frac{bc}{bd}=\frac{c}{d},$$

所以$\frac{0}{b}$是零元素,简记作0.

容易验证,$\frac{a}{b}$的负元素是$\frac{(-a)}{b}$.

因为

$$\frac{b}{b}\cdot\frac{c}{d}=\frac{bc}{bd}=\frac{c}{d},$$

所以$\frac{b}{b}$是单位元素,简记作1.

设$\frac{a}{b}\neq 0$,即$\frac{a}{b}\neq\frac{0}{b}$,则$a\neq 0$,从而存在$\frac{b}{a}$,并且

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=1.$$

因此$\frac{a}{b}$可逆,并且$\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$.

综上所述得,F是一个域.令

$$\sigma: R \longrightarrow F$$

$$a \longmapsto \frac{a}{1},$$

容易验证,σ是环R到F的一个单同态.因此F可看成是R的一个扩环,可以把a与$\sigma(a)$等同.于是

$$\frac{a}{b}=\frac{a}{1}\cdot\frac{1}{b}=\frac{a}{1}\cdot\left(\frac{b}{1}\right)^{-1}=\sigma(a)[\sigma(b)]^{-1}=ab^{-1}.$$

这表明F是R的一个分式域.

定理 1　设 R 是一个整环，则存在 R 的分式域，并且在同构的意义下，R 的分式域是唯一的.

证明　存在性已证.下面证唯一性.

设 F 和 F' 都是 R 的分式域，则存在 R 到 F 的一个单同态 σ，存在 R 到 F' 的一个单同态 σ'.令

$$\begin{aligned}\psi:\ & F \longrightarrow F' \\ & \sigma(a)\sigma(b)^{-1} \longmapsto \sigma'(a)\sigma'(b)^{-1}.\end{aligned} \tag{7}$$

$$\begin{aligned}&\sigma(a)\sigma(b)^{-1} = \sigma(x)\sigma(y)^{-1}\\ &\Longleftrightarrow \sigma(a)\sigma(y) = \sigma(x)\sigma(b)\\ &\Longleftrightarrow \sigma(ay) = \sigma(xb)\\ &\Longleftrightarrow ay = xb\\ &\Longleftrightarrow \sigma'(ay) = \sigma'(xb)\\ &\Longleftrightarrow \sigma'(a)\sigma'(b)^{-1} = \sigma'(x)\sigma'(y)^{-1}.\end{aligned}$$

因此 ψ 是 F 到 F' 的一个映射，并且是单射.

任取 F' 的一个元素 $\sigma'(a)\sigma'(b)^{-1}$，其中 $a \in R, b \in R^*$，则 $\sigma(a)\sigma(b)^{-1} \in F$，并且据 ψ 的定义得，$\psi[\sigma(a)\sigma(b)^{-1}] = \sigma'(a)\sigma'(b)^{-1}$.因此 ψ 是满射.

容易直接验证 ψ 保持加法和乘法运算，因此 ψ 是 F 到 F' 的一个同构.从而 $F \cong F'$.　□

* 习题 2.5

*1. 设 R 为一个有单位元 $1(\neq 0)$ 的交换环，R 的一个非空子集 S 称为**乘性子集**(multiplicative subset)，如果 S 对乘法封闭(即若 $s_1, s_2 \in S$，则 $s_1s_2 \in S$)，且 $1 \in S$.

令 $I = \{a \in R \mid 存在 s \in S 使得 as = 0\}$.

(1) 证明 I 是 R 的一个理想；

(2) 如果 $0 \in S$，则 $I = R$；如果 $0 \notin S$，则 $I \cap S = \varnothing$；如果 S 不含 R 的零因子，则 $I = (0)$.

*2. 设 R 和 R' 都是有单位元的交换环，且 $1 \neq 0, 1' \neq 0'$. 设 S 是 R 的一个乘性子集，I 是第 1 题所定义的 R 的理想. 如果存在环 R 到 R' 的一个同态 σ，使得对任意 $s \in S$ 都有 $\sigma(s)$ 在 R' 内可逆；$\operatorname{Ker}\sigma = I$；并且 R' 的每个元素 x 可表示成 $x = \sigma(a)\sigma(s)^{-1}$，其中 $a \in R, s \in S$，则 R' 称为 R 关于乘性子集 S 的**分式环**(ring of fractions).

证明：如果 $0 \notin S$，则存在 R 关于乘性子集 S 的分式环.（注：当 R 为整环时，如果取 $S = R^*$，则 $S^{-1}R$ 就是 R 的分式域.）

*3. 设 p 是 $\mathbf{Z}$ 中一个素数，令 $S = \mathbf{Z} - (p)$. 证明：S 是 $\mathbf{Z}$ 的一个乘性子集；$I = (0)$；整数 a 在 $S^{-1}\mathbf{Z}$ 中可逆当且仅当 a 与 p 互素；$S^{-1}\mathbf{Z}$ 的元素可写成

$$x = \frac{r}{s} \cdot p^t,$$

其中 $r, s \in \mathbf{Z}, (rs, p) = 1, t \in \mathbf{N}$；$x$ 可逆当且仅当 $t = 0$.

§6　唯一因子分解整环，主理想整环，欧几里得整环

我们已经知道，整数环 $\mathbf{Z}$ 的结构：每一个正整数可以唯一地分解成有限多个素数的乘积(除了素数的排列次序外)；域 F 上一元多项式环 $F[x]$ 的结构：每一个次数大于 0 的多项式可以分解成有限多个不可约多项式的乘积，而且在相伴的意义下这种分解方式是唯一的. 整数环 $\mathbf{Z}$ 和域 F 上的一元多项式环 $F[x]$ 都是整环. 自然会问：对于任意一个整环 R，有没有类似于 $\mathbf{Z}$ 和 $F[x]$ 这样的结构？本节就来探讨这一问题. 本节的环 R 都是整环，不再每次声明.

设 R 是一个整环. 任意取定 $a, b \in R$，如果存在 $c \in R$，使得 $a = bc$，则称 b **整除** a，记作 $b \mid a$. 此时称 b 是 a 的**因子**(factor 或 divisor)，a 是 b 的**倍数**(multiple).

$b \mid a$ 当且仅当 $(b) \supseteq (a)$.

整除关系具有反身性和传递性，但是没有对称性.

u 是 R 的单位（即可逆元）当且仅当 $u \mid 1$，从而 $(u) = R$.

R 的单位 u 是 R 中每一个元素 a 的因子，这是因为 $a = u(u^{-1}a)$.

如果 $b \mid a_1$ 且 $b \mid a_2$，则 $b \mid (r_1a_1 + r_2a_2)$，$\forall r_1, r_2 \in R$.

如果 $a \mid b$ 且 $b \mid a$，则称 a 与 b **相伴**(associates)，记作 $a \sim b$.

相伴是等价关系.

$a \sim b$ 当且仅当 $(a) = (b)$.

$a \sim b$ 当且仅当有 R 的单位 u 使得 $a = bu$. 理由如下：设 $a \sim b$，则存在 $u, v \in R$，使得 $b = av, a = bu$. 若 $a = 0$，则 $b = 0$，从而结论成立. 若 $a \neq 0$，由上述式子得，$a = avu$. 两边消去 a，得 $1 = vu$. 因此 u 是 R 的单位. 反之，如果有 R 的单位 u 使得 $a = bu$，则显然有 $a \sim b$.

如果 $a \sim b, c \sim d$，则 $ac \sim bd$（由上一结论可立即推出此结论）.

如果 $b \mid a$，但是 $a \nmid b$（即 b 是 a 的因子，但 b 不是 a 的相伴元），则称 b 是 a 的一个**真因子**(proper factor). 不难看出，若 u 是单位，则 u 没有真因子.

R 中，任一单位，以及 a 的任一相伴元都称为 a 的**平凡因子**(trivial factors). a 的其它因子（如果还有的话）称为 a 的非平凡因子.

定义 1　设 $a \in R$，如果 $a \neq 0$，a 不是单位，并且 a 只有平凡因子，则称 a 是**不可约的**(irreducible)；否则，称 a 是**可约的**(reducible).

不可约元的相伴元也是不可约元（可直接验证）.

定义 2　设 $a \in R$，$a \neq 0$，且 a 不是单位. 如果从 $a \mid bc$ 可以推出 $a \mid b$ 或 $a \mid c$，则称 a 是一个**素元**(prime element).

命题 1　在整环 R 中，每一个素元一定是不可约元.

证明　设 a 是 R 的一个素元. 任取 a 的一个因子 b, 则存在 $c \in R$, 使得 $a = bc$. 于是 $a \mid bc$. 从而 $a \mid b$ 或 $a \mid c$. 如果 $a \mid b$, 则 $a \sim b$. 如果 $a \mid c$, 则存在 $d \in R$, 使得 $c = ad$. 从而 $a = bc = bad$. 由于 $a \neq 0$, 因此 $1 = bd$. 于是 b 为单位. 综合上述得, a 是一个不可约元. □

命题 1 的逆命题不成立. 即整环 R 中不可约元不一定是素元. 我们在本节习题第 1 题给出例子.

命题 2　在整环 R 中, a 为素元当且仅当 (a) 为非零素理想.

证明　a 为素元

$\Longleftrightarrow a \neq 0$, a 不是单位且从 $a \mid bc$ 可推出 $a \mid b$ 或 $a \mid c$

$\Longleftrightarrow (a) \neq (0)$, $(a) \neq R$ 且从 $bc \in (a)$ 可推出 $b \in (a)$ 或 $c \in (a)$

$\Longleftrightarrow (a)$ 为非零素理想 □

从命题 2 可得出, 在整环 R 里, 如果元素 a 生成的理想 (a) 为非零极大理想, 则 a 为素元. 再据命题 1 得, a 为不可约元.

设 $a, b \in R$, 如果有 $c \in R$, 使得 $c \mid a$ 且 $c \mid b$, 则称 c 是 a 与 b 的**公因子**(common divisor). a 与 b 的一个公因子 d 称为**最大公因子**(greatest common divisor), 如果从 $c \mid a$, $c \mid b$ 可推出 $c \mid d$.

如果 d_1, d_2 都是 a 与 b 的最大公因子, 则从定义立即得出, $d_1 \sim d_2$. 我们用 (a, b) 表示 a 与 b 的任何一个确定的最大公因子.

在整环 R 中, 不一定每一对元素都有最大公因子. 可以参看本节习题第 1 题.

引理　在整环 R 中, 如果每一对元素都有最大公因子, 则对任意 $a, b, c \in R$, 有 $(ca, cb) \sim c(a, b)$.

证明　如果 $c = 0$, 则显然有 $(ca, cb) \sim c(a, b)$. 如果 $(a, b) = 0$, , 则从 $0 \mid a$ 且 $0 \mid b$ 推出 $a = 0$ 且 $b = 0$, 从而 $(ca, cb) \sim c(a, b)$. 下面设 $c \neq 0$ 且 $(a, b) \neq 0$. 记 $d = (a, b)$, $e = (ca, cb)$. 由于 $d \mid a$ 且 $d \mid b$, 因此 $cd \mid ca$ 且 $cd \mid cb$, 从而 $cd \mid (ca, cb)$, 即 $cd \mid e$. 于是存在 $u \in R$, 使得 $e = cdu$. 我们来证明 u 是单位. 由于 $e \mid ca$, 因此存在 $v \in$

R,使得 $ca = ev$,从而 $ca = cduv$. 消去 c,得 $a = duv$. 同理 $b = duv'$. 因此 $du \mid (a,b)$,即 $du \mid d$. 从而存在 $u' \in R$,使得 $d = duu'$. 由于 $d \neq 0$,消去 d 得,$1 = uu'$. 因此 u 是单位. 从而 $e \sim cd$. □

定义 3 整环 R 如果满足下列两个条件:

(1) R 中每一个非零且非单位的元素 a 可以分解成有限多个不可约元的积:$a = p_1p_2\cdots p_s$;

(2) 上述分解在相伴的意义下是唯一的,即如果 a 有两个这样的分解式:

$$a = p_1p_2\cdots p_s, \quad a = q_1q_2\cdots q_t,$$

则 $t = s$,并且将 q_i 的下标适当改为可使得

$$p_i \sim q_i, \quad i = 1,2,\cdots,s.$$

那么我们称 R 是一个**唯一因子分解整环**(unique factorization domain),或者**高斯整环**(Gaussian domain).

从本节习题第 1 题可看出,并非每一个整环都是唯一因子分解整环. 下面我们来探讨整环 R 应当满足什么条件才是唯一因子分解整环.

定理 3 设 R 是唯一因子分解整环,则

(i) R 的每一对元素都有最大公因子;

(ii) R 的每一个不可约元都是素元;

(iii) 因子链条件(divisor chain condition)成立,即如果序列 a_1, a_2, a_3, $\cdots$ 中,每一个 a_i 是 a_{i-1} 的真因子,则这个序列是有限序列.

证明 (i) 任取 $a,b \in R$,若 $a = 0$,则 $b = (0,b)$. 若 a 是单位,则 $a = (a,b)$. 下面设 a,b 都是非零且非单位. 因为 R 是唯一因子分解整环,所以有两两不相伴的不可约元 $p_1, p_2, \cdots, p_s$,以及单位 u,v,使得

$$a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}, \quad \alpha_i \geqslant 0, \quad 1 \leqslant i \leqslant s,$$

$$b = vp_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}, \quad \beta_i \geqslant 0, \quad 1 \leqslant i \leqslant s,$$

其中至少有一个 $\alpha_j > 0$，$\beta_j > 0$. 令

$$d = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_s^{\min\{\alpha_s,\beta_s\}},$$

则 $d \mid a$ 且 $d \mid b$.

如果 c 是 a 与 b 的一个公因子，则

$$c = u' p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}, \quad \gamma_i \leqslant \min\{\alpha_i, \beta_i\}, \quad 1 \leqslant i \leqslant s.$$

因此 $c \mid d$. 这就证明了 $d = (a, b)$.

(ii) 设 p 是 R 的不可约元. 设 $p \mid bc$. 由于 p 只有平凡的因子，因此 $(p, b) \sim p$ 或者 (p, b) 是单位. 如果 $(p, b) \sim p$，则 $p \mid b$. 如果 (p, b) 是单位，则

$$(cp, cb) \sim c(p, b) \sim c.$$

由于 $p \mid bc$ 且 $p \mid cp$，因此 $p \mid (cp, cb)$，从而 $p \mid C$. 综上所述得，p 是一个素元.

(iii) 如果 a_1 是单位，则 a_1 没有真因子，从而序列中只有一项 a_1. 显然 0 的真因子是非零元，因此下面不妨设 $a_1 \neq 0$ 且 a_1 非单位. 从而存在有限多个两两不相伴的不可约元 $p_1, p_2, \cdots, p_s$，使得

$$a_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad 1 \leqslant i \leqslant s.$$

a 的任一因子形如 $vp_1^{m_1} p_2^{m_2} \cdots p_s^{m_s}$，$0 \leqslant m_i \leqslant \alpha_i$，$1 \leqslant i \leqslant s$，$v$ 是单位. 对应于 $(m_1, m_2, \cdots, m_s)$ 的两种不同的取法，所得到的 a_1 的两个因子是不相伴的(因为它们至少相差一个不可约元). 因此 a_1 的两两不相伴的因子只有有限多个. 从而序列 $a_1, a_2, a_3, \cdots$ 是有限序列(因为每一个 a_i 都是 a_{i-1} 的真因子，所以序列中任意两项都是 a_1 的不相伴的因子.) □

定理 4 整环 R 如果满足下列两个条件：

(i) 因子链条件，

(ii) 每一个不可约元都是素元，

则 R 是唯一因子分解整环.

证明 设 a 是 R 中非零且非单位的一个元素. 如果 a 不可约,则 $a=a$. 下面设 a 可约,则 a 有真因子. 先证 a 有一个真因子是不可约的. 设 a_1 是 a 的一个真因子. 若 a_1 不可约,则 a_1 就是所要找的. 若 a_1 可约,则 a_1 有真因子 a_2. 若 a_2 不可约,则易看出 a_2 是 a 的一个真因子,从而 a_2 是所要找的. 若 a_2 可约,则 a_2 有真因子 a_3. 如此下去,得到序列

$$a, a_1, a_2, a_3, \cdots \tag{1}$$

其中每个元素是前面一个的真因子. 由于 R 满足因子链条件,因此(1)是有限序列. 设它的最后一项为 a_n. 则 a_n 是不可约的. 易看出 a_n 是 a 的真因子,把 a_n 记作 p_1,于是 $a=p_1c_1$. 从而 c_1 是 a 的真因子. 若 c_1 不可约,则 a 分解成了两个不可约元 p 和 c_1 的乘积. 若 c_1 可约,显然 c_1 非零且非单位,由前面的讨论知道,c_1 有真因子 p_2 不可约,于是 $c_1=p_2c_2$,从而 c_2 是 c_1 的真因子. 如此下去,得到序列

$$a, c_1, c_2, \cdots \tag{2}$$

其中每一个元素是前面一个的真因子,由因子链条件,序列(2)有限. 设序列(2)终止于 c_{s-1}. 于是 c_{s-1} 不可约. 记 c_{s-1} 为 p_s,则

$$a=p_1c_1=p_1p_2c_2=\cdots=p_1p_2\cdots p_{s-1}c_{s-1}=p_1p_2\cdots p_{s-1}p_s.$$

下面来证唯一性,设 a 有两种这样的分解:

$$a=p_1p_2\cdots p_s,\quad a=q_1q_2\cdots q_t. \tag{3}$$

对第一种分解式中的不可约元的个数 s 作数学归纳法.

$s=1$ 时,$a=p_1=q_1q_2\cdots q_t$. 假如 $t>1$,则

$$p_1=q_1(q_2\cdots q_t).$$

因为 p_1 不可约,所以 q_1 是 p_1 的平凡因子,由于 q_1 不是单位,因此 $q_1\sim p_1$. 于是 $q_1=p_1u$,其中 u 为单位. 从而

$$p_1=p_1u(q_2\cdots q_t).$$

由此推出,$1=u(q_2\cdots q_t)$. 从而 q_2 是单位,矛盾. 因此 $t=1$. 于是 $p_1=q_1$.

假设分解式中不可约元的个数为 $s-1$ 时唯一性成立，来看不可约元的个数为 s 的情形.

由于 p_1 不可约，根据已知条件(ii)得，p_1 为素元. 于是从 $p_1 \mid q_1q_2\cdots q_t$ 可推出 p_1 整除某个 q_j. 通过改写 q_j 的下标可设 $p_1 \mid q_1$. 由于 q_1 不可约，因此 $p_1 \sim q_1$. 于是 $p_1 = q_1 v$，其中 v 是单位. 从而

$$q_1 v p_2 \cdots p_s = q_1 q_2 \cdots q_t.$$

两边消去 q_1，得 $(vp_2)\cdots p_s = q_2\cdots q_t$. 由归纳假设得，$s-1=t-1$，即 $s=t$；并且适当改写 q_j 的下标可以使 $vp_2 \sim q_2, p_3 \sim q_3, \cdots, p_s \sim q_s$，从而有

$$p_i \sim q_i, \quad i = 1,2,\cdots,s.$$

根据数学归纳法原理，唯一性得证.

综上所述得，R 为唯一因子分解整环. □

推论 5 整环 R 如果满足下列两个条件：

(i) 因子链条件；

(ii) 每一对元素都有最大公因子，

则 R 为唯一因子分解整环.

证明 从定理 3 的(ii)的证明过程知道，如果 R 中每一对元素都有最大公因子，则 R 中每一个不可约元都是素元. 从而由定理 4 立即得出，R 为唯一因子分解整环. □

我们知道，整数环 $\mathbf{Z}$ 和域 F 上一元多项式环 $F[x]$ 的每一个理想都是主理想.

定义 4 一个整环 R 称为**主理想整环**(principal ideal domain)，如果 R 的每个理想都是主理想.

$\mathbf{Z}$ 和 $F[x]$ 都是主理想整环，它们也都是唯一因子分解整环. 那么主理想整环与唯一因子分解整环之间有什么关系？

我们已经知道，在整环 R 中，如果 (a) 是非零极大理想，则 a 是不可约元. 反之不然. 例如，在 $\mathbf{Z}[x]$ 中，容易看出，x 是不可约多项

式;而在本章 §3 我们已证明(x)不是极大理想.但是我们将证明在主理想整环中,不可约元生成的理想一定是极大理想.

定理 6 设 R 为主理想整环,则

(i) 不可约元 p 生成的理想(p)一定是极大理想;

(ii) R 为唯一因子分解整环.

证明 (i) 设 p 为不可约元,则 $p\neq 0$ 且 p 非单位.于是$(p)\neq(0)$且$(p)\neq R$.设 R 的理想 $I\supseteq(p)$,因为 R 是主理想整环,所以 $I=(a)$.从$(a)\supseteq(p)$得出 $a\mid p$.由于 p 只有平凡的因子,因此 $a\sim p$ 或 a 是单位.如果 $a\sim p$,则$(a)=(p)$.如果 a 是单位,则$(a)=R$.因此(p)是 R 的极大理想.

(ii) 据(i),若 p 为不可约元,则(p)是非零极大理想,从而(p)是非零素理想.因此 p 是素元.

R 中任取一个序列 $a_1,a_2,a_3,\cdots$,其中每个 a_i 是 a_{i-1} 的真因子.于是$(a_i)\supsetneqq(a_{i-1})$.从而

$$(a_1)\subsetneqq(a_2)\subsetneqq(a_3)\cdots$$

令 $I=\bigcup_i(a_i)$.容易验证 I 是 R 的一个理想.由于 R 是主理想环,因此 $I=(d)$.由于 $d\in\bigcup_i(a_i)$,因此 d 属于某个(a_j).从而 $a_j\mid d$.于是$(a_j)\supseteq(d)$.又$(a_j)\subseteq(d)$,因此$(a_j)=(d)=I$.如果序列 $a_1,a_2,a_3,\cdots,a_j,\cdots$ 有第 $j+1$ 项 a_{j+1},则$(a_{j+1})\supsetneqq(a_j)=I$.矛盾.因此该序列终止于 a_j,即它是有限序列,从而 R 满足因子链条件.

综上所述得,R 是唯一因子分解整环. □

我们知道,整数环 $\mathbf{Z}$ 和域 F 上的一元多项式环 $F[x]$ 都有带余除法.由此受到启发,我们引出下述概念:

定义 5 设 R 为一个整环,如果存在 R^* 到自然数集 $\mathbf{N}$ 的一个映射 δ,使得对任意 $a,b\in R$ 且 $b\neq 0$,都有 $h,r\in R$ 满足

$$a=hb+r,\quad r=0\text{ 或 }r\neq 0\text{ 且 }\delta(r)<\delta(b),$$

则称 R 是一个**欧几里得整环**(Euclidean domain).

定理 7　欧几里得整环都是主理想整环.

证明　设 R 是欧几里得整环. 任取 R 的一个理想 I 且设 $I \neq (0)$. 取 I 的一个非零元 b, 使得

$$\delta(b) \leqslant \delta(x), \quad \forall x \in I \setminus \{0\}.$$

显然 $(b) \subseteq I$. 反之, 设 $a \in I$, 由于 R 是欧几里得整环, 因此存在 h, $r \in R$, 使得

$$a = hb + r, \ r = 0 \text{ 或 } r \neq 0 \text{ 且 } \delta(r) < \delta(b).$$

倘如 $r \neq 0$, 则 $r = a - hb \in I$, 这与 b 的取法矛盾. 因此 $r = 0$, 从而 $a = hb \in (b)$. 因此 $I = (b)$. □

整数环 $\mathbf{Z}$ 是唯一因子分解整环, 即 $\mathbf{Z}$ 是高斯整环. 试问: $\mathbf{Z}$ 上的一元多项式环 $\mathbf{Z}[x]$ 是不是高斯整环呢? 我们来探讨这一问题.

任取 $f(x) \in \mathbf{Z}[x]$, 且 $f(x) \neq 0$. 设 $f(x)$ 的各项系数的最大公因子为 d, 则 $f(x) = df_1(x)$, 其中 $f_1(x)$ 的各项系数的最大公因子为 ± 1, 此时称 $f_1(x)$ 是一个**本原多项式**(primitive polynomial).

我们在高等代数课程中证明了下列结论的(1) – (4)(可参看丘维声编著《高等代数(第二版) 下册》(高等教育出版社 2003 年出版) 第七章 §8 的引理 1, 引理 2, 定理 1, 定理 3):

(1) 两个本原多项式 $g(x)$ 与 $h(x)$ 在 $\mathbf{Q}[x]$ 中相伴当且仅当 $g(x) = \pm h(x)$.

(2) **高斯引理**. 两个本原多项式的乘积还是本原多项式.

(3) 次数大于 0 的本原多项式 $g(x)$ 在 $\mathbf{Q}$ 上可约当且仅当 $g(x)$ 可以分解成两个次数都比 $g(x)$ 的次数低的本原多项式的乘积.

(4) 每一个次数大于 0 的本原多项式 $g(x)$ 可以唯一地分解成 $\mathbf{Q}$ 上不可约的本原多项式的乘积.

(5) 一个次数大于 0 的本原多项式 $g(x)$ 在 $\mathbf{Q}$ 上不可约当且仅当它在 $\mathbf{Z}$ 上不可约(充分性由上述结论(3) 立即得出; 必要性用反证法容易得出.)

(6) 从上述最后两个结论立即得出, 每一个次数大于 0 的本原

多项式 $g(x)$ 可以唯一地分解成 $\mathbf{Z}$ 上不可约的本原多项式的乘积.

现在任取 $f(x)\in\mathbf{Z}[x]$,且 $\deg f(x)>0$,则 $f(x)=df_1(x)$,其中 d 是 $f(x)$ 的各项系数的最大公因子,从而 $f_1(x)$ 是本原多项式.据上述结论,$f_1(x)$ 可以唯一地分解成 $\mathbf{Z}$ 上不可约的本原多项式的乘积,如果 $d\neq\pm 1$,则 d 可以唯一地分解成一些素数的乘积.因此 $f(x)$ 可以唯一地分解成 $\mathbf{Z}[x]$ 中一些不可约元的乘积,这就证明了 $\mathbf{Z}[x]$ 是唯一因子分解整环.即 $\mathbf{Z}[x]$ 是高斯整环.

上述证明 $\mathbf{Z}[x]$ 是高斯整环的方法也可用于证明下述结论:

定理 8 高斯整环 R 上的一元多项式环 $R[x]$ 也是高斯整环.

由定理 8 以及 $R[x_1,x_2,\cdots,x_n]=R[x_1][x_2]\cdots[x_n]$ 立即得出:

推论 9 高斯整环 R 上的 n 元多项式环 $R[x_1,x_2,\cdots,x_n]$ 也是高斯整环.

据推论 9 得,$\mathbf{Z}[x_1,x_2,\cdots,x_n]$ 是高斯整环,其中 n 是任意正整数.

高等代数课讲了判别次数大于 0 的整系数多项式 $f(x)$ 在 $\mathbf{Q}[x]$ 中不可约的一种方法:Eisenstein 判别法.类似地可证明:

定理 10(Eisenstein 判别法) 设 F 为一个高斯整环 R 的分式域.设

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in R[x],\quad a_n\neq 0,n>1.$$

如果 R 有一个不可约元 p 满足:

(1) $p\mid a_i,i=0,1,\cdots,n-1$;

(2) $p\nmid a_n$,且 $p^2\nmid a_0$,

则 $f(x)$ 在 $F[x]$ 中不可约.

在本章 §1 我们讲了域 F 上的 n 元多项式环 $F[x_1,x_2,\cdots,x_n]$ 中,一组多项式 $\{f_i(x_1,x_2,\cdots,x_n)\}$ 的公共零点集称为 F^n 的一个代数簇,记作 $V(\{f_i\})$.

设 C 是 F^n 的一个代数簇，我们考虑零点集包含 C 的所有多项式组成的集合：

$$I = \{f(x_1,x_2,\cdots,x_n) \mid f(c_1,c_2,\cdots,c_n) = 0,\ \forall (c_1,c_2,\cdots,c_n) \in C\}$$

显然 I 是 $F[x_1,x_2,\cdots,x_n]$ 的一个理想. 因此研究 F^n 的代数簇归结为研究 $F[x_1,x_2,\cdots,x_n]$ 的理想. 自然要问：I 是不是由有限多个多项式生成的？

定理 11 设 R 是一个交换环，则 R 的每一个理想是有限生成的当且仅当 R 满足**理想的升链条件**(ascending chain condition for ideals). 即 R 的每一条理想升链

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots$$

都有限. 也就是说，存在一个正整数 m，使得

$$I_m = I_{m+1} = I_{m+2} = \cdots.$$

证明 必要性. 假设 R 不满足理想升链条件，即存在一个理想的序列

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots \tag{4}$$

是无限的，令 $I = \bigcup_i I_i$，易看出 I 是 R 的一个理想. 由已知条件，可设 I 是由 $\{a_1,a_2,\cdots,a_n\}$ 生成的. 则 $a_1 \in I_{j_1}$ 对某个 j_1，$a_2 \in I_{j_2}$ 对某个 j_2，$\cdots$，$a_n \in I_{j_n}$ 对某个 j_n. 于是 $I \subseteq \bigcup_{i=1}^{n} I_{j_i}$. 又有 $I \supseteq \bigcup_{i=1}^{n} I_{j_i}$. 因此 $I = \bigcup_{i=1}^{n} I_{j_i}$. 这表明序列(4)到 I_{j_n} 终止，矛盾. 因此 R 满足理想升链条件.

充分性. 设 R 满足理想升链条件. 假如 R 有一个理想 I 是无限生成的，则能找到 I 中元素的序列

$$a_1,a_2,a_3,\cdots$$

使得

$$(a_1) \subsetneqq (a_1,a_2) \subsetneqq (a_1,a_2,a_3) \subsetneqq \cdots.$$

这个理想的升链是无限的,矛盾.因此 R 的每一个理想是有限生成的. □

定义 6 如果一个交换环 R 满足理想升链条件,则 R 称为**诺特环**(Noether ring).

Emmy Noether(1882—1935) 是德国数学家, 她是 Max Noether(1844—1921) 的女儿. M. Noether 对代数几何作出了奠基性工作. E. Noether 是发展现代理想理论的中心人物.

定理 12(希尔伯特基定理 Hilbert Basis Theorem) 如果 R 是一个有单位元 $1(\neq 0)$ 的诺特环,则 R 上的一元多项式环 $R[x]$ 也是诺特环.

证明 设 U 是 $R[x]$ 的任一理想.设 I 由 U 中所有非零多项式的首项系数连同 0 组成的集合,我们来证明 I 是 R 的一个理想.对于 $a,b \in I$,则存在 $f(x),g(x) \in U$,使得 $f(x) = ax^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $g(x) = bx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ 都属于 U.不妨设 $n \geqslant m$.于是 $f(x) - x^{n-m}g(x) \in U$.如果 $a = b$,则 $a - b = 0 \in I$;如果 $a \neq b$,则 $a - b$ 是 $f(x) - x^{n-m}g(x)$ 的首项系数,从而 $a - b \in I$.设 $a \in I, r \in R$.如果 $ra \neq 0$,则 $rf(x)$ 的首项系数为 $ra \in I$;如果 $ra = 0$,则 $ra = 0 \in I$.因此 I 是 R 的一个理想.

因为 R 是诺特环,所以 I 是有限生成的.设 $I = (a_1, a_2, \cdots, a_s)$,其中 a_i 是 U 中多项式 $f_i(x)$ 的首项系数,$1 \leqslant i \leqslant s$.设 $m = \max\{\deg f_1(x), \cdots, \deg f_s(x)\}$.

对每一个 $k(0 \leqslant k < m)$,令 I_k 是由 U 中次数小于或等于 k 的所有多项式的首项系数连同 0 组成的集合.类似于证明 I 为理想的方法,可证明 I_k 是 R 的理想.由于 R 是诺特环,因此可设

$$I_k = (a_{k1}, a_{k2}, \cdots, a_{kr_k}), \quad k = 0, 1, \cdots, m-1.$$

其中 a_{kj} 是 U 中多项式 g_{kj} 的首项系数.我们断言

$$U = (f_1(x), \cdots, f_s(x), g_{11}(x), \cdots, g_{m-1, r_{m-1}}(x)). \qquad (5)$$

(5) 式右端的理想记作 $\mathscr{U}'$. 显然 $\mathscr{U}' \subseteq \mathscr{U}$. 假如 $\mathscr{U}' \subsetneqq \mathscr{U}$, 设 $h(x)$ 是属于 $\mathscr{U}$ 但不属于 $\mathscr{U}'$ 的次数最低的多项式.

情形 1　设 $\deg h(x) = l \geqslant m$, 记 $\deg f_i(x) = l_i, 1 \leqslant i \leqslant s$. 从 I 的定义知道, 可以把 $h(x)$ 的首项系数 a 写成 $a = \sum_{i=1}^{s} r_i a_i$, 其中 $r_i \in R, 1 \leqslant i \leqslant s$. 于是多项式 $\sum_{i=1}^{s} r_i x^{l-l_i} f_i(x)$ 的首项系数为 $\sum_{i=1}^{s} r_i a_i = a$, 首项为 ax^l. 从而有

$$\deg\left(\sum_{i=1}^{s} r_i x^{l-l_i} f_i(x) - h(x)\right) < l. \tag{6}$$

显然 $\sum_{i=1}^{s} r_i x^{l-l_i} f_i(x) - h(x) \in \mathscr{U}$. 由 $h(x)$ 的选取和(6)式知,

$$\sum_{i=1}^{s} r_i x^{l-l_i} f_i(x) - h(x) \in \mathscr{U}' \tag{7}$$

由于 $f_i(x) \in \mathscr{U}', 1 \leqslant i \leqslant s$, 因此从(7)式推出, $h(x) \in \mathscr{U}'$, 矛盾.

情形 2　设 $\deg h(x) = l < m$, 记 $\deg g_{kj} = n_{kj}$. 从 I_l 的定义知道, 可设 $h(x)$ 的首项系数 $a = \sum_{j=1}^{v_l} r_{lj} a_{lj}$. 于是多项式 $\sum_{j=1}^{v_l} r_{lj} x^{l-n_{lj}} g_{lj}(x)$ 的首项系数为 $\sum_{j=1}^{v_l} r_{lj} a_{lj} = a$, 首项为 ax^l. 从而 $\deg\left(\sum_{j=1}^{v_l} r_{lj} x^{l-n_{lj}} g_{lj}(x) - h(x)\right) < l$. 与情形 1 的最后议论类似, 由此推出 $h(x) \in \mathscr{U}'$, 矛盾.

综上所述得, $\mathscr{U}' = \mathscr{U}$, 即 $\mathscr{U}$ 是有限生成的. 据定理 11 得, $R[x]$ 是诺特环. □

由定理 12 以及 $R[x_1, x_2, \cdots, x_n] = R[x_1][x_2]\cdots[x_n]$ 立即得到:

推论 13　如果 R 是有单位元 $1(\neq 0)$ 的诺特环, 则 R 上的 n 元

多项式环 $R[x_1, x_2, \cdots, x_n]$ 也是诺特环，$n \in \mathbf{Z}^+$. □

由于域 F 只有平凡的理想：(0) 和 $F = (1)$，因此 F 是诺特环. 从而 $F[x_1, x_2, \cdots, x_n]$ 是诺特环，因此 $F[x_1, x_2, \cdots, x_n]$ 的每一个理想都是有限生成的. 这个结论在代数几何中起着重要作用.

由于 $\mathbf{Z}$ 的每个理想都是主理想，因此 $\mathbf{Z}$ 是诺特环. 于是 $\mathbf{Z}[x_1, x_2, \cdots, x_n]$ 也是诺特环.

习题 2.6

1. 设 $R = \mathbf{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbf{Z}\}$. 对于 $\alpha = a + b\sqrt{-5}$，规定 $N(\alpha) \xlongequal{\text{def}} \alpha\bar{\alpha} = a^2 + 5b^2$，称 $N(\alpha)$ 是 α 的**范数**(norm).

(1) 证明：α 是 $\mathbf{Z}[\sqrt{-5}]$ 的单位当且仅当 $N(\alpha) = 1$；并且求出 $\mathbf{Z}[\sqrt{-5}]$ 的所有单位；

(2) 证明：如果 $N(\alpha) = 9$，则 α 是不可约元；说明 3 和 $2 \pm \sqrt{-5}$ 都是不可约元；

(3) 证明：3 和 $2 \pm \sqrt{-5}$ 都不是素元；

(4) 证明 $\mathbf{Z}[\sqrt{-5}]$ 不是唯一因子分解整环；

*(5) 证明 9 和 $6 + 3\sqrt{-5}$ 没有最大公因子.

2. $\mathbf{Z}[x]$ 是唯一因子分解整环. 证明：$(2, x^2 + 1)$ 不是主理想，从而 $\mathbf{Z}[x]$ 不是主理想整环.

*3. 证明高斯整数环 $\mathbf{Z}[\sqrt{-1}]$ 是欧几里特整环.

4. 设 m 是一个没有平方因子的整数且 $m \neq 0, 1$. 证明 $\mathbf{Q}[\sqrt{m}]$ 是一个域，它的元素形如 $a + b\sqrt{m}$, $a, b \in \mathbf{Q}$.

5. 设 m 是一个没有平方因子的整数且 $m \neq 0, 1$. 在 $\mathbf{Q}[\sqrt{m}]$ 中，定义子集 R 如下：

当 $m \equiv 2$ 或 $3 \pmod 4$ 时，$R = \{a + b\sqrt{m} \mid a, b \in \mathbf{Z}\}$，

当 $m\equiv 1 \pmod 4$ 时，$R=\left\{a+b\cdot\frac{1+\sqrt{m}}{2}\,\middle|\, a,b\in\mathbf{Z}\right\}$.

证明 R 是 $\mathbf{Q}[\sqrt{m}]$ 的一个子环. 今后把上述 R 分别记作 $\mathbf{Z}[\sqrt{m}]$, $\mathbf{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. R 称为 $\mathbf{Q}[\sqrt{m}]$ 的**代数整数环**(ring of algebraic integers).

第三章　域扩张及其自同构

§1　域扩张，分裂域，有限域的结构，正规扩张

在第二章的 §3 和 §4，我们讲了从一个域 F 出发，通过在 F 的一元多项式环 $F[x]$ 中找一个不可约多项式 $m(x)$，作商环 $F[x]/(m(x))$，便得到一个域 $F[x]/(m(x))$. 我们还以有理数域 $\mathbf{Q}$ 为例，通过 $\mathbf{Q}$ 添加一个代数数 t，便得到一个域 $\mathbf{Q}[t]$，它同构于 $\mathbf{Q}[x]/(p(x))$，其中 $p(x)$ 是 t 在 $\mathbf{Q}$ 上的极小多项式. 这种构造域的方法也适用于任意一个域 F. 设 R' 是 F 的一个扩环，且 R' 是交换环. 如果 R' 的一个元素 α 在 F 上是代数的，则存在 $F[x]$ 中的非零多项式以 α 为根. $F[x]$ 中以 α 为根的所有非零多项式中，取一个次数最低的且首项系数为 1 的多项式 $m(x)$，称 $m(x)$ 是 α 在 F 上的**极小多项式**. 容易看出，$m(x)$ 一定是 $F[x]$ 中的不可约多项式. 于是有 $F[x]/(m(x)) \cong F[\alpha]$，从而 $F[\alpha]$ 是一个域. 当 $F[\alpha]$ 是域时，把它记成 $F(\alpha)$.

上面两种方法都使我们可以从一个域 F 出发，构造一个比 F 大的域. 这称为域扩张. 本章要研究域扩张的性质、结构及其应用.

定义 1　设 F 和 K 都是域，并且 F 是 K 的一个子环，则称 F 是 K 的一个**子域**(subfield)，称 K 是 F 的一个**扩域**(extension field)，或者称 K 是 F 上的**域扩张**(field extension)，记作 K/F. K 的包含 F 的任一子域称为 K/F 的**中间域**(intermediate field).

容易看出，域 K 的单位元素 e 通过加法生成 K 的一个子环

$$K_0 = \{ne \mid n \in \mathbf{Z}\}.$$

当 K 的特征为 0 时，$K_0 \cong \mathbf{Z}$，因为 K_0 的分式域与有理数域 $\mathbf{Q}$ 同构，将 ne^{-1} 与 n 等同，则 $\mathbf{Q}$ 可看作 K 的子域．此时称 $\mathbf{Q}$ 是 K 的**素域**(prime field)．

当 K 的特征为 p 时，

$$K_0 \cong \mathbf{Z}_p.$$

于是 $\mathbf{Z}_p$ 可看成 K 的子域．此时称 $\mathbf{Z}_p$ 是 K 的**素域**．

如果域 F 到域 K 有一个单的环同态，则 K 可以看成是 F 的一个扩域．

如果 F 的域扩张 K/F 可以在 F 上添加一个元素 α 得到：$K = F(\alpha)$，则称 K 是 F 上的一个**单扩张**(simple extension)．

像上面讲的域 F 添加它的扩环 R' 里的一个代数元 α 得到的域 $F(\alpha)$ 是 F 的单扩张．如果 α' 是 α 在 F 上的极小多项式 $m(x)$ 在 R' 中的另一个根(此时容易看出，$m(x)$ 也是 α' 在 F 上的极小多项式)，则同理有

$$F[x]/(m(x)) \cong F[\alpha'].$$

从而 $F[\alpha']$ 也是域，把 $F[\alpha']$ 记成 $F(\alpha')$．于是有

$$F(\alpha) \cong F(\alpha'),$$

并且有一个同构映射 η 满足 $\eta(\alpha) = \alpha'$，以及 $\eta(a) = a$，$\forall a \in F$．

如果给了 $F[x]$ 的一个不可约多项式 $m(x)$，则商环 $F[x]/(m(x))$ 是一个域．由于 F 到 $F[x]/(m(x))$ 有一个单的环同态，因此 $F[x]/(m(x))$ 可以看成是 F 的一个扩域．令 $u = x + (m(x))$，则 $m(u) = 0$．因此 u 是 $m(x)$ 在 $F[x]/(m(x))$ 中的一个根．此时有 $F[x]/(m(x)) = F[u]$．把 $F[u]$ 记成 $F(u)$．如果 u' 是 $m(x)$ 在 $F[x]/(m(x))$ 中的另一个根，则 u' 是 F 上的一个代数元，且 u' 在 F 上的极小多项式是 $m(x)$．据上一段知，

$$F[x]/(m(x)) \cong F[u'].$$

从而 $F[u']$ 也是域，并且有

$$F[u] \cong F[u'],$$

其同构映射 ψ 满足 $\psi(u) = u'$，$\psi(a) = a$，$\forall a \in F$.

现在我们从另一个角度研究域扩张，这可帮助我们揭示域扩张的一些内在性质. 因此这是研究域扩张的一条重要途径.

设 K/F 是一个域扩张，则 K 可以看成是域 F 上的一个线性空间，它的加法运算是域 K 中的加法，它的纯量乘法运算是域 F 的元素与 K 的元素做 K 中的乘法运算. K 作为域 F 上的线性空间的维数称为 K 在 F 上的**次数**(degree of K over F)，记作 $[K:F]$. 如果 $[K:F]$ 是有限的，则称 K 是 F 上的**有限扩张**(finite extension). 此时 K 作为 F 上的线性空间的一个基也叫做域扩张 K/F 的一个**基**(basis). 利用这个看法，我们可以揭示域扩张的下列性质.

定理 1 设 K/F 为有限扩张，则 K 的每个元素都是 F 上的代数元.

证明 设 $[K:F] = n$，任取 $\beta \in K$，则 $1, \beta, \beta^2, \cdots, \beta^n$ 在 F 上必线性相关，从而存在 F 中不全为 0 的元素 $a_0, a_1, \cdots, a_n$，使得

$$a_0 + a_1\beta + a_2\beta^2 + \cdots + a_n\beta^n = 0.$$

令 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$，则 $f(\beta) = 0$. 由于 $f(x) \neq 0$，因此 β 在 F 上是代数的. □

域扩张 K/F 称为**代数扩张**(algebraic extension)，如果 K 的每一个元素都是 F 上的代数元.

定理 1 表明，有限扩张一定是代数扩张.

定理 2 设 K/F 是域扩张，$\alpha \in K$ 且 α 是 F 上的代数元. 如果 α 在 F 上的极小多项式 $m(x)$ 的次数为 n，则

$$[F(\alpha):F] = n,$$

并且 $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ 是 $F(\alpha)/F$ 的一个基.

证明 假如 $1, \alpha, \cdots, \alpha^{n-1}$ 在 F 上线性相关，则有 F 中不全为 0

的元素 $b_0,b_1,\cdots,b_{n-1}$ 使得

$$b_0+b_1\alpha+\cdots+b_{n-1}\alpha^{n-1}=0.$$

令 $g(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}$.则 $g(\alpha)=0$.这与 $m(x)$ 是以 α 为根的次数最低的非零多项式矛盾.因此,$1,\alpha,\cdots,\alpha^{n-1}$ 线性无关.又由于

$$F(\alpha)=F[\alpha]=\{c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}\mid c_i\in F,0\leqslant i<n\},$$

因此 $1,\alpha,\cdots,\alpha^{n-1}$ 是 $F(\alpha)/F$ 的一个基.于是$[F(\alpha):F]=n$. □

定理2表明,域 F 添加一个代数元 α 得到的单扩张 $F(\alpha)$ 一定是有限扩张,从而它是代数扩张.于是称 $F(\alpha)/F$ 是**单代数扩张**(simple algebraic extension).

域 F 添加一个超越元 t 得到的单扩张 $F(t)$ 称为**单超越扩张**(simple transcendental extension).不难证明,$F(t)$ 同构于 $F[x]$ 的分式域(即域 F 上的一元有理函数域).

定理3 设有三个域:$K\supseteq L\supseteq F$,则$[K:F]$有限当且仅当$[K:L]$和$[L:F]$都有限,此时有

$$[K:F]=[K:L][L:F]. \tag{1}$$

证明 必要性.设$[K:F]$有限,由于 L 是 K 的一个子空间,因此$[L:F]$有限.设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是线性空间 K/F 的一个基,任取 $\beta\in K$,有

$$\beta=\sum_{i=1}^{n}b_i\alpha_i,\quad b_i\in F,\quad i=1,2,\cdots,n.$$

由于 $F\subseteq L$,因此 $b_i\in L,1\leqslant i\leqslant n$.从而 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是域 L 上线性空间 K 的一组生成元.因此$[K:L]$有限.

充分性.设$[K:L]=m$,$[L:F]=s$.设 $\beta_1,\beta_2,\cdots,\beta_m$ 和 $\gamma_1,\gamma_2,\cdots,\gamma_s$ 分别是 K/L 和 L/F 的一个基.任取 $\alpha\in K$,有

$$\alpha=\sum_{i=1}^{m}a_i\beta_i,\quad a_i\in L,i=1,2,\cdots,m.$$

从而有

$$a_i = \sum_{j=1}^{s} b_{ij}\gamma_j, \quad b_{ij} \in F, 1 \leqslant j \leqslant s, \ i = 1,2,\cdots,m.$$

因此

$$\alpha = \sum_{i=1}^{m}\sum_{j=1}^{s} b_{ij}(\gamma_j\beta_i). \tag{2}$$

容易验证,K 的子集

$$\{\gamma_j\beta_i \mid 1 \leqslant i \leqslant m, \ 1 \leqslant j \leqslant s\} \tag{3}$$

在 F 上线性无关,因此子集(3)就是 K 在 F 上的一个基. 于是 $[K:F] = ms = [K:L][L:F]$. ∎

历史上研究域扩张的推动力来自研究代数方程可用根式求解的条件,伽罗瓦(Galois)于1830年前后彻底解决了这一问题. 他的想法的出发点是,把数域 F 上代数方程 $f(x) = 0$ 左端多项式 $f(x)$ 的所有复根与 F 一起,形成复数域 $\mathbf{C}$ 的一个子域,而且使这个子域是包含 F 和 $f(x)$ 的所有复根的域中最小的一个. 从这个想法引出下列概念:

定义 2 设 K/F 是一个域扩张,S 是 K 的一个非空子集. 我们把 K 中包含 F 和 S 的一切子域的交称为 **F 添加 S 得到的子域**,或 **S 在 F 上生成的子域**,记作 $F(S)$. 如果 $S = \{a_1, a_2, \cdots, a_n\}$,则把 $F(S)$ 写成 $F(a_1, a_2, \cdots, a_n)$.

显然,$F(S)$ 是域 K 里包含 F 和 S 的所有子域中最小的一个.

设 $\alpha \in K$,则 $F[\alpha]$ 表示 K 中包含 F 和 α 的所有子环的交. $F(\alpha)$ 表示 K 中包含 F 和 α 的所有子域的交. 容易看出,当 $F[\alpha]$ 是子域时,必有

$$F[\alpha] = F(\alpha).$$

我们在本节开头说,当 $F[\alpha]$ 是域时,把它记成 $F(\alpha)$,其道理就是这里所讲的.

定义 3 设 $f(x)$ 是域 F 上的一个 $n(n \geqslant 1)$ 次多项式. 如果有一个域扩张 E/F 满足

(i) $f(x)$ 在 E 内完全分解成一次因式的乘积

$$f(x)=c(x-a_1)(x-a_2)\cdots(x-a_n),\quad a_i\in E,\quad 1\leqslant i\leqslant n;$$

(ii) $E=F(a_1,a_2,\cdots,a_n)$,

则 E/F 称为 $f(x)$ 在 F 上的一个**分裂域**(splitting field).

如果 F 是一个数域,则定义 3 中的条件(i)表明 E 包含了 $f(x)$ 的所有复根,而条件(ii)表明 E 是包含 $f(x)$ 的全部复根的最小的子域.

任给一个域 F 上的多项式 $f(x)$,它在 F 上的分裂域是否存在?如果存在,是否唯一?为了探究这些问题,我们首先对于定义 2 中的 $F(a_1,a_2,\cdots,a_n)$ 稍作一点调查.

由于 $F(a_1,\cdots,a_{n-1})(a_n)$ 是 K 中包含 $F(a_1,\cdots,a_{n-1})$ 和 a_n 的一切子域的交,因此

$$F(a_1,\cdots,a_{n-1})(a_n)\subseteq F(a_1,\cdots,a_{n-1},a_n).\tag{4}$$

又由于 $F(a_1,\cdots,a_{n-1})(a_n)$ 是 K 中包含 F 和 $a_1,\cdots,a_{n-1},a_n$ 的一个子域,因此

$$F(a_1,\cdots,a_{n-1})(a_n)\supseteq F(a_1,\cdots,a_{n-1},a_n).\tag{5}$$

于是从(4)、(5)两式得

$$F(a_1,\cdots,a_{n-1},a_n)=F(a_1,\cdots,a_{n-1})(a_n).\tag{6}$$

运用数学归纳法容易得出

$$F(a_1,\cdots,a_{n-1},a_n)=F(a_1)(a_2)\cdots(a_{n-1})(a_n).\tag{7}$$

从(7)式又可得出

$$F(a_1,\cdots,a_r,b_1,\cdots,b_s)=F(a_1,\cdots,a_r)(b_1,\cdots,b_s).\tag{8}$$

定理 4 任一域 F 上每一个 $n(n\geqslant 1)$ 次多项式 $f(x)$ 在 F 上有一个分裂域 E,并且 $[E:F]\leqslant n!$.

证明 对多项式的次数 n 作数学归纳法. $n=1$ 时,$f(x)=c(x-a)$,$a\in F$. 于是 F 本身是 $f(x)$ 的一个分裂域,且 $[F:F]=1\leqslant 1!$.

假设次数 r 小于 n 的多项式有分裂域,且其分裂域对 F 的次数 $\leqslant r!$.现在来看 n 次多项式 $f(x)$. 任取 $f(x)$ 的一个不可约因式 $p(x)$. 我们知道 $F[x]/(p(x))$ 是一个域. 令 $\alpha_1 = x + (p(x))$,则 $F[x]/(p(x)) = F[\alpha_1] = F(\alpha_1)$,并且 $p(\alpha_1) = 0$. 从而 $f(\alpha_1) = 0$. 记 $E_1 = F(\alpha_1)$. 则可设

$$f(x) = (x - \alpha_1)\cdots(x - \alpha_l)f_1(x), \quad \alpha_i \in E_1, \quad 1 \leqslant i \leqslant l,$$

其中 $f_1(x) \in E_1[x]$. 如果 $\deg f_1(x) = 0$,则容易看出 E_1 就是 $f(x)$ 在 F 上的一个分裂域. 下设 $\deg f_1(x) \geqslant 1$. 由于 $\deg f_1(x) = n - l < n$,根据归纳假设,$f_1(x)$ 在 E_1 上有一个分裂域 E,并且 $[E:E_1] \leqslant (n-l)! \leqslant (n-1)!$. 于是

$$f_1(x) = c(x - \beta_1)\cdots(x - \beta_{n-l}), \quad \beta_j \in E, \quad 1 \leqslant j \leqslant n - l,$$

并且 $E = E_1(\beta_1, \cdots, \beta_{n-l})$. 从而

$$f(x) = c(x - \alpha_1)\cdots(x - \alpha_l)(x - \beta_1)\cdots(x - \beta_{n-l}).$$

并且 $E = F(\alpha_1)(\beta_1, \cdots, \beta_{n-l})$. 由于 $\alpha_i \in E_1$, $1 \leqslant i \leqslant l$,因此 $F(\alpha_1, \cdots, \alpha_l) \subseteq E_1 = F(\alpha_1)$. 显然 $F(\alpha_1, \cdots, \alpha_l) \supseteq F(\alpha_1)$. 于是

$$E = F(\alpha_1, \cdots, \alpha_l)(\beta_1, \cdots, \beta_{n-l}) = F(\alpha_1, \cdots, \alpha_l, \beta_1, \cdots, \beta_{n-l}).$$

因此 E 是 $f(x)$ 在 F 上的一个分裂域,并且

$$\begin{aligned}[E:F] &= [E:E_1][E_1:F] \leqslant (n-1)!\deg(p(x)) \\ &\leqslant (n-1)!n = n!\end{aligned}$$

根据数学归纳法原理,对于一切 $n \geqslant 1$,命题成立. □

我们想证明 $f(x)$ 的分裂域在同构的意义下是唯一的. 为了以后的应用,我们来证明更一般的结论.

定理 5 设域 F 到域 F' 有一个同构 σ. 设 $F[x]$ 中的 $n(n \geqslant 1)$ 次多项式 $f(x) = \sum_{i=0}^{n} a_i x^i$ 在 F 上的一个分裂域是 E. 令 $f^{\sigma}(x) = \sum_{i=0}^{n} \sigma(a_i)x^i \in F'[x]$,并且设 $f^{\sigma}(x)$ 在 F' 上的一个分裂域是 E',则 σ 可以开拓成域 E 到 E' 的一个同构.

证明 对次数$[E:F]$作数学归纳法. 当$[E:F]=1$时, $E=F$. 从而

$$f(x)=c(x-a_1)(x-a_2)\cdots(x-a_n),\quad a_i\in F,\quad 1\leqslant i\leqslant n.$$

于是

$$f^{\sigma}(x)=\sigma(c)[(x-\sigma(a_1)][(x-\sigma(a_2)]\cdots[(x-\sigma(a_n)],$$
$$\sigma(a_i)\in F',\quad 1\leqslant i\leqslant n.$$

这表明E'是$f^{\sigma}(x)$在F'上的一个分裂域, 从而$E'=F'$. 因此σ已经是E到E'的一个同构.

假设$[E:F]<m$时, 命题成立, 其中$m>1$. 现在来看$[E:F]=m$的情形. 因为$m>1$, 所以$f(x)$有一个次数大于1的不可约因式$p(x)$(否则, $f(x)$在$F[x]$中已经分解成n个一次因式的乘积, 这与$[E:F]=m>1$矛盾). 设$\alpha_1\in E$是$p(x)$的一个根. 则$[F(\alpha_1):F]=r>1$, 其中$r=\deg p(x)$. 显然α_1是$f(x)$的一个根. 由于E是$f(x)$在F上的一个分裂域, 因此

$$f(x)=c(x-\alpha_1)\cdots(x-\alpha_l)(x-\beta_1)\cdots(x-\beta_{n-l}),$$

其中$\alpha_i\in F(\alpha_1)$, $1\leqslant i\leqslant l$; $\beta_j\in E$, 且$\beta_j\notin F(\alpha_1)$, $1\leqslant j\leqslant n-l$. 由于$f(x)$也可看成是$F(\alpha_1)$上的一个多项式, 并且

$$\begin{aligned}E&=F(\alpha_1,\cdots,\alpha_l,\beta_1,\cdots,\beta_{n-l})\\&=F(\alpha_1,\cdots,\alpha_l)(\beta_1,\cdots,\beta_{n-l})\\&=F(\alpha_1)(\beta_1,\cdots,\beta_{n-l}).\end{aligned}$$

因此E是$f(x)$在$F(\alpha_1)$上的一个分裂域.

由于$p(x)$在$F[x]$中不可约, 因此容易看出$p^{\sigma}(x)$在$F'[x]$中不可约, 且$\deg p^{\sigma}(x)=\deg p(x)=r$. 设$\beta_1$是$p^{\sigma}(x)$在$E'$中的一个根. 同上面的道理, E'是$f^{\sigma}(x)$在$F'(\beta_1)$上的一个分裂域. 令

$$\sigma_1:\ F(\alpha_1)\longrightarrow F'(\beta_1)$$
$$\sum_{i=0}^{r-1}a_i\alpha_1^i\longmapsto\sum_{i=0}^{r-1}\sigma(a_i)\beta_1^i,$$

由于 $F[\alpha_1]/F$ 的一个基是 $1,\alpha_1,\cdots,\alpha_1^{l-1}$,因此 σ_1 是映射.由于 $F'(\beta_1)/F$ 的一个基是 $1,\beta_1,\cdots,\beta_1^{l-1}$,因此 σ_1 是满射和单射.容易直接验证 σ_1 保持加法和乘法,从而 σ_1 是域 $F(\alpha_1)$ 到 $F'(\beta_1)$ 的一个同构.由于

$$[E:F]=[E:F(\alpha_1)][F(\alpha_1):F]>[E:F(\alpha_1)],$$

因此 $[E:F(\alpha_1)]<m$.根据归纳假设,域 $F(\alpha_1)$ 到域 $F'(\beta_1)$ 的同构 σ_1 可以开拓成域 E 到 E' 的一个同构.

根据数学归纳法原理,命题得证. □

推论6 设 $f(x)$ 是域 F 上的 $n(n\geqslant 1)$ 次多项式,E 和 E' 都是 $f(x)$ 在 F 上的分裂域,则 $E\cong E'$,且存在 E 到 E' 的一个同构 η,使得 η 在 F 上的限制 $\eta|F$ 为恒等映射.

证明 在定理5中,取 $F'=F$,取 σ 为 F 上的恒等映射,则 σ 可开拓成 E 到 E' 的一个同构 η.从定理5的证明过程看出,$\eta|F$ 是恒等映射. □

定义4 设 K_1/F 和 K_2/F 是两个域扩张,如果存在域 K_1 到 K_2 的一个同构(或同态)η,使得 η 在 F 上的限制 $\eta|F$ 为恒等映射,则称 η 为一个 **$F-$同构**(或 **$F-$同态**).

注:(1) 如果 $f(x)\in F[x]$ 的两个分裂域 E 和 E' 是 F 的同一个扩域 K 的两个子域,则 $E=E'$.理由如下:我们有

$$f(x)=c(x-\alpha_1)\cdots(x-\alpha_n),\quad \alpha_i\in E,\quad 1\leqslant i\leqslant n,\tag{9}$$

$$f(x)=d(x-\beta_1)\cdots(x-\beta_n),\quad \beta_i\in E',\quad 1\leqslant i\leqslant n.\tag{10}$$

由于 $E\subseteq K$,$E'\subseteq K$,因此(9)、(10)式都是 $f(x)$ 在 $K[x]$ 中的因式分解,由于 $K[x]$ 是唯一因子分解整环,因此 $c=d$,且 $\beta_1,\beta_2,\cdots,\beta_n$ 是 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的一个排列.从而

$$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\beta_1,\beta_2,\cdots,\beta_n)=E'.$$

(2) 如果域扩张 K/F 的一个中间域 E/F 是一个多项式 $f(x)\in$

$F[x]$ 的分裂域，则 E 在 K 的任意一个 F – 自同构 η 下保持不变，即 $\eta(E)=E$. 理由如下：由于

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),\quad \alpha_i\in E,\quad 1\leqslant i\leqslant n, \tag{11}$$

且 η 是 K 的一个 F – 自同构，因此据一元多项式的根与系数的关系可得

$$f^{\eta}(x)=c(x-\eta(\alpha_1))(x-\eta(\alpha_2))\cdots(x-\eta(\alpha_n)), \tag{12}$$

其中 $\eta(\alpha_i)\in\eta(E), 1\leqslant i\leqslant n$. 设 $f(x)=\sum_{i=0}^{n-1}a_ix^i$，则

$$f^{\eta}(x)=\sum_{i=0}^{n-1}\eta(a_i)x^i=\sum_{i=0}^{n-1}a_ix^i=f(x).$$

于是从(12)式看出，$f(x)$ 在 $\eta(E)$ 上完全分解成一次因式的乘积. 又由于 $E=F(\alpha_1,\cdots,\alpha_n)$，因此 $\eta(E)=F(\eta(\alpha_1),\cdots,\eta(\alpha_n))$. 从而 $\eta(E)$ 是 $f(x)$ 在 F 上的一个分裂域. 由于 E 和 $\eta(E)$ 都是 K 的子域，据注(1)的结论得，$\eta(E)=E$.

现在我们运用分裂域的理论来研究有限域的结构. 我们在第二章 §3 讲了构造有限域的一种方法. 设 $q=p^n$，p 为素数. 在 $\mathbf{Z}_p[x]$ 中找一个 n 次不可约多项式 $m(x)$，则 $\mathbf{Z}_p[x]/(m(x))$ 是一个含 p^n 个元素的有限域. 令 $u=x+(m(x))$，则

$$\begin{aligned}&\mathbf{Z}_p[x]/(m(x))\\&=\{c_0+c_1u+\cdots+c_{n-1}u^{n-1}\mid c_i\in\mathbf{Z}_p,0\leqslant i<n\}\\&=\mathbf{Z}_p[u]=\mathbf{Z}_p(u).\end{aligned}$$

上述构造有限域的方法是非常好的. 不过我们要问：对于任意素数 p，任意正整数 n，在 $\mathbf{Z}_p[x]$ 中一定存在 n 次不可约多项式吗？回答是肯定的，而且还可以求出 $\mathbf{Z}_p[x]$ 中首项系数为 1 的 n 次不可约多项式的个数 $\mathbf{N}_p(n)$（参看 R. Lidl 和 H. Niederreiter 著《Introduction to finite fields and their applications (Revised edition)》第 86 页的定理 3.25，Cambridge University Press，1994 年）. 这表明 p^n 元有限域是

一定存在的．下面我们想用另一种方法证明有限域的存在性，同时可以揭示 p^n 元有限域的唯一性．产生这另一种方法的想法来源如下：上述 q 元有限域 $\mathbf{Z}_p(u)$ 的乘法群是 $q-1$ 阶循环群，于是它的每一个元素 α 满足 $\alpha^{q-1}=1$，从而 $\alpha^q=\alpha$．因此 $\mathbf{Z}_p(u)$ 的每一个元素都是 $\mathbf{Z}_p[x]$ 中的多项式 x^q-x 的根．于是 $\mathbf{Z}_p(u)$ 包含了 x^q-x 的全部根．由此得出，$\mathbf{Z}_p(u)$ 是 x^q-x 在 $\mathbf{Z}_p$ 上的一个分裂域．这就产生了证明 q 元有限域存在的另一种方法．

定理 7 设 $q=p^n$，p 为素数，则 q 元有限域一定存在，并且任意两个 q 元有限域都是同构的．

证明 存在性．据定理 4，$\mathbf{Z}_p[x]$ 中的多项式 x^q-x 在 $\mathbf{Z}_p$ 上有一个分裂域 E．则 x^q-x 在 E 内恰好有 q 个根．由于

$$(x^q-x)'=qx^{q-1}-1=-1,$$

因此 $(x^q-x,(x^q-x)')=1$，从而 x^q-x 没有重因式（可参看丘维声编著《高等代数（下册）》第154页第2题的第(5)小题）．因此 x^q-x 的 q 个根两两不同．设它们为 $\alpha_1,\alpha_2,\cdots,\alpha_q$．则 $E=\mathbf{Z}_p(\alpha_1,\alpha_2,\cdots,\alpha_q)$．令

$$K=\{\alpha_1,\alpha_2,\cdots,\alpha_q\}.$$

由于

$$(\alpha_i-\alpha_j)^q=\alpha_i^q-\alpha_j^q=\alpha_i-\alpha_j,$$

$$(\alpha_i\alpha_j^{-1})^q=\alpha_i^q(\alpha_j^q)^{-1}=\alpha_i\alpha_j^{-1}，当\ \alpha_j\neq 0.$$

因此 $\alpha_i-\alpha_j\in K$；$\alpha_i\alpha_j^{-1}\in K$，当 $\alpha_j\neq 0$．从而 K 是 E 的子域．由于 $\bar{1}\in K$，因此 $\mathbf{Z}_p$ 中任一元素 $\bar{i}=i\bar{1}\in K$，从而 K 是包含 $\mathbf{Z}_p$ 和 $\alpha_1,\alpha_2,\cdots,\alpha_q$ 的一个域．于是

$$K\supseteq\mathbf{Z}_p(\alpha_1,\alpha_2,\cdots,\alpha_q)=E.$$

由此推出，$K=E$．这证明了 E 是含 q 个元素的域，它是 $\mathbf{Z}_p[x]$ 中多项式 x^q-x 在 $\mathbf{Z}_p$ 上的一个分裂域．

唯一性．设 F 是任意一个 q 元有限域，用 e 表示 F 的单位元素．由

于 $q=p^n$，因此 F 的特征是 p. 令

$$F_p=\{0,e,2e,\cdots,(p-1)e\}.$$

容易验证 F_p 是 F 的一个子域(称 F_p 是 F 的素域). 下面也用 1 表示 F 的单位元，由于 F^* 是 $q-1$ 阶循环群，因此 F^* 中每一个元素 α 满足 $\alpha^{q-1}=1$，从而 $\alpha^q=\alpha$. 于是 F 的全部元素是 $F_p[x]$ 中多项式 x^q-x 在 F 中全部根. 因此 F 是 x^q-x 在 F_p 上的一个分裂域. 容易验证，$\sigma: i\mapsto ie$ 是 $\mathbf{Z}_p$ 到 F_p 的一个同构. 记 $f(x)=x^q-x\in\mathbf{Z}_p[x]$，则 $f^\sigma(x)=x^q-x\in F_p[x]$，据定理 5 得，$\sigma$ 可以开拓成 E 到 F 的一个同构. 因此 $E\cong F$. 再据同构的对称性和传递性得，任意两个 q 元有限域都有同构. □

对于 $q=p^n$，p 为素数，由于任意两个 q 元有限域都同构. 因此我们可以用 F_q 表示 q 元有限域，或者记作 $GF(q)$. 有限域也称为**伽罗瓦域**(Galois fields)，因为有限域是由伽罗瓦首先提出的.

域 F 上的一个 $n(n\geqslant 1)$ 次多项式 $f(x)$ 的分裂域 E 是一个域扩张 E/F，使得 $f(x)$ 在 E 内完全分解成一次因式的乘积. 我们知道，$f(x)$ 首先可以分解成 $F[x]$ 中的一些不可约多项式的乘积：$f(x)=p_1(x)p_2(x)\cdots p_s(x)$(其中 $p_i(x),i=1,2,\cdots,s$ 不必不同). 既然 $f(x)$ 在 E 内能完全分解成一次因式的乘积，那么当然每一个 $p_i(x)(i=1,2,\cdots,s)$ 也可以在 E 内完全分解成一次因式的乘积. 由此再大胆设想一下：可不可能找到 F 的一扩域 K，使得 $F[x]$ 中任意一个在 K 中有根的不可约多项式都可以在 $K[x]$ 中完全分解成一次因式的乘积？我们来探讨这个问题. 首先给这种扩域 K 取一个名字：

定义 5 一个代数扩张 K/F 称为**正规扩张**(normal extension)，如果 $F[x]$ 的任一在 K 中有根的不可约多项式都可以在 $K[x]$ 中完全分解成一次因式的乘积.

我们有下述结论：

定理 8 一个有限扩张 K/F 是正规扩张当且仅当 K 为 $F[x]$ 的一个多项式的分裂域.

证明 必要性. 设 K/F 是一个有限正规扩张. 如果 $[K:F]=1$，则 $K=F$，没什么可证的. 下面设 $[K:F]>1$. 于是存在 $\alpha_1\in K$，但 $\alpha_1 \notin F$. 令 $F_1=F(\alpha_1)$，则 F_1/F 是单代数扩张，且 $[F_1:F]>1$. 据定理 3 得，$[K:F_1]<[K:F]$. 从而可以用第二数学归纳法证明，K/F 有一个中间域的有限升链：

$$F=F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \cdots \subsetneqq F_{s-1} \subsetneqq F_s=K,$$

使得 F_{i+1}/F_i 为单代数扩张，$i=0,1,\cdots,s-1$. 从而存在 $\alpha_1,\alpha_2,\cdots,\alpha_s\in K$，使得

$$K=F(\alpha_1)(\alpha_2)\cdots(\alpha_{s-1})(\alpha_s)=F(\alpha_1,\alpha_2,\cdots,\alpha_{s-1},\alpha_s),$$

其中 α_i 是 F 上的代数元，$i=1,2,\cdots,s$. 设 $p_i(x)$ 是 α_i 在 F 上的极小多项式，$\alpha=1,2,\cdots,s$. 令

$$f(x)=p_1(x)p_2(x)\cdots p_s(x).$$

由于 K/F 是正规扩张，因此每个不可约多项式 $p_i(x)$ 在 $K[x]$ 中能完全分解成一次因式的乘积. 从而 $f(x)$ 在 $K[x]$ 中也能完全分解成一次因式的乘积：

$$f(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n).$$

于是 $\beta_i\in K$，$i=1,2,\cdots,n$. 从而 $F(\beta_1,\beta_2,\cdots,\beta_n)\subseteq K$. 由于 α_i 是 $p_i(x)$ 在 K 中的根，当然也是 $f(x)$ 在 K 中的根，$i=1,2,\cdots,s$. 因此 $\{\alpha_1,\alpha_2,\cdots,\alpha_s\}\subseteq\{\beta_1,\beta_2,\cdots,\beta_n\}$. 从而

$$K=F(\alpha_1,\alpha_2,\cdots,\alpha_s)\subseteq F(\beta_1,\beta_2,\cdots,\beta_n).$$

综上所述得，$K=F(\beta_1,\beta_2,\cdots,\beta_n)$. 据分裂域的定义得出，$K$ 是 $f(x)$ 的分裂域.

充分性. 设 K/F 是域 F 的一个 $n(n\geqslant 1)$ 次多项式 $f(x)$ 的分裂域. 设 $p(x)$ 是 $F[x]$ 中一个不可约多项式，且 $p(x)$ 在 K 中有一个根 α. 我们来证 $p(x)$ 在 $K[x]$ 中能完全分解成一次因式的乘积. 设

E/K 是 $p(x)$ 在 K 上的分裂域. 容易看出 E/F 是 $g(x)=f(x)p(x)$ 在 F 上的分裂域. 设 β 是 $p(x)$ 在 E 中的任一根, 则 $F(\alpha)\cong F(\beta)$, 并且有一个同构映射 η 满足 $\eta(\alpha)=\beta$, 以及 $\eta(a)=a$, $\forall a\in F$. 根据定理5, η 可以开拓成 $p(x)$ 在 $F(\alpha)$ 上的分裂域 E 到 $p(x)$ 在 $F(\beta)$ 上的分裂域 E 的一个 F-同构 σ, 即 E 的一个 F-自同构 σ, 因为 K/F 是 $f(x)$ 的分裂域, 且 K/F 是 E/F 的一个中间域, 据上面的注(2)得, $\sigma(K)=K$. 由于 $\alpha\in K$, 因此 $\beta=\eta(\alpha)=\sigma(\alpha)\in K$. 这证明了 $p(x)$ 在 $K[x]$ 中就可完全分解成一次因式的乘积. 从而 K/F 是正规扩张. □

下面我们介绍域扩张理论中与多项式有无重根有关的概念.

定义 6　$F[x]$ 中一个不可约多项式 $p(x)$ 称为**可分的**(separable), 如果 $p(x)$ 在它的分裂域内只有单根. $F[x]$ 中一个次数大于0的多项式 $f(x)$ 称为**可分的**, 如果它的每一个不可约因式是可分的. 换句话说, 无重根的多项式称为可分多项式.

定义 7　设 K/F 是一个域扩张, $\alpha\in K$ 是 F 上的一个代数元. 如果 α 的极小多项式是**可分的**, 则称 α 是在 F 上可分的; 否则, 称 α 是在 F 上**不可分的**.

定义 8　一个代数扩张 K/F 称为**可分扩张**(separable extension), 如果 K 的每一个元素在 F 上都是可分的; 否则, 称 K/F 是**不可分扩张**.

定理 9　一个有限扩张 E/F 是可分正规扩张当且仅当 E 是 F 上一个可分多项式的分裂域.

证明可看聂灵沼、丁石孙著《代数学引论(第二版)》第 222 页定理 11 的证明.

习题 3.1

1. 设 K/F 是一个域扩张, $\alpha,\beta\in K$ 且 α,β 是 F 上的代数元, 证

明:$\alpha \pm \beta, \alpha\beta, \alpha\beta^{-1}(\beta \neq 0)$ 都是 F 上的代数元;从而 K 里 F 上的所有代数元组成一个子域,称这个域是 F 在 K 中的**代数闭包**,记作 $\bar{F}$.

2. 求 $\mathbf{Q}[x]$ 中下列多项式在 $\mathbf{Q}$ 上的分裂域,并且求分裂域在 $\mathbf{Q}$ 上的次数:

(1) $f(x) = (x^2 - 2)(x^2 - 3)$; (2) $f(x) = x^4 - 2$.

3. 设 q 是素数 p 的方幂,且 $GF(q^l)$ 是 $GF(q^m)$ 的子域.

(1) 证明 l 是 m 的因子;

(2) 设 f 是域 $GF(q^l)$ 上线性空间 $GF(q^m)$ 的一个非零线性函数. 对于 $\alpha \in GF(q^m)$,定义 $f_\alpha(\beta) = f(\alpha\beta), \forall \beta \in GF(q^m)$. 证明: $GF(q^m)$ 的每一个线性函数形如 f_α,并且当 $\alpha \neq \gamma$ 时,$f_\alpha \neq f_\gamma$.

§2 域扩张的自同构,伽罗瓦群,伽罗瓦扩张

Galois 理论是通过域扩张的自同构来研究域扩张. 一个基本目的是,说明在适当条件下一个 n 次扩张恰好有 n 个自同构.

设 σ 是域 E 到域 E' 的一个同态,则 σ 当然也是 E 的加法群到 E' 的加法群的同态. 在 E 到 E' 的所有(加法)群同态组成的集合 Ω 中,规定

$$(\sigma_i + \sigma_j)x \xlongequal{\text{def}} \sigma_i(x) + \sigma_j(x), \quad \forall x \in E,$$

$$(k\sigma)x \xlongequal{\text{def}} k\sigma(x), \quad \forall x \in E,$$

其中 $k \in E'$. 容易验证,Ω 对于上述加法和纯量乘法成为域 E' 上的一个线性空间,其中零元素为 E 到 E' 的零映射:$x \longmapsto 0', \forall x \in E$,这个零映射是 E 的加法群到 E' 的加法群的同态,但它不是 E 到 E' 的环同态(因为它把 E 的单位元 1 映成了 E' 的零元).

引理 1(Dedekind 引理) 域 E 到域 E' 的不同的同态组成的任一集合是在域 E' 上线性无关的.

证明 设 $\{\sigma_i \mid i \in I\}$ 是域 E 到域 E' 的一族不同的同态,它们也

都可看成是(加法)群同态.如果它们在域 E' 上线性相关,则有一个有限子集是线性相关的.取元素数目最少的线性相关的有限子集

$$\{\sigma_1, \sigma_2, \cdots, \sigma_r\},$$

并且设 σ_1 可以由其余向量线性表出,即 $\sigma_1 = \sum_{i=2}^{r} k_i\sigma_i, k_i \in E', 2 \leqslant i \leqslant r$.从而

$$\sigma_1(x) = \left(\sum_{i=2}^{r} k_i\sigma_i\right)x = \sum_{i=2}^{r} k_i\sigma_i(x), \quad \forall x \in E. \tag{1}$$

在(1)式中用 xy 代替 x,得

$$\sigma_1(xy) = \sum_{i=2}^{r} k_i\sigma_i(xy), \quad \forall x, y \in E.$$

由于 σ_i 是环同态,因此有

$$\sigma_1(x)\sigma_1(y) = \sum_{i=2}^{r} k_i\sigma_i(x)\sigma_i(y), \quad \forall x, y \in E. \tag{2}$$

用 $\sigma_1(y)$ 乘(1)式两边,且从(2)式减去这结果,得

$$0 = \sum_{i=2}^{r} k_i\sigma_i(x)[\sigma_i(y) - \sigma_1(y)], \quad \forall x, y \in E. \tag{3}$$

即
$$0 = \left\{\sum_{i=2}^{r} k_i[\sigma_i(y) - \sigma_1(y)]\sigma_i\right\}x, \quad \forall x, y \in E.$$

于是

$$\sum_{i=2}^{r} k_i[\sigma_i(y) - \sigma_1(y)]\sigma_i = 0, \quad \forall y \in E. \tag{4}$$

由于 $\{\sigma_1, \sigma_2, \cdots, \sigma_r\}$ 是最小的线性相关的有限子集,因此 $\sigma_2, \cdots, \sigma_r$ 线性无关.于是从(4)式得

$$k_i[\sigma_i(y) - \sigma_1(y)] = 0, \quad \forall y \in E,\ i = 2, \cdots, r. \tag{5}$$

因为 $\sigma_i \neq \sigma_1 (2 \leqslant i \leqslant r)$,所以存在 $y \in E$,使得 $\sigma_i(y) \neq \sigma_1(y)$.从而由(5)式,得 $k_i = 0, i = 2, \cdots, r$.由此得出,

$$\sigma_1 = \sum_{i=2}^{r} k_i\sigma_i = 0.$$

这与 σ_1 是环同态矛盾.因此 $\{\sigma_i \mid i \in I\}$ 是在 E' 上线性无关的. □

定理 1 设 E 和 E' 是域 F 的两个扩张.如果 $[E:F]=n$,则存在至多 n 个从 E 到 E' 的 F - 同态.

证明 设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 E/F 的一个基.假如存在 $n+1$ 个从 E 到 E' 的不同的 F - 同态 $\sigma_0,\sigma_1,\cdots,\sigma_n$.则域 E' 上 $n+1$ 个未知量 $x_0,x_1,\cdots,x_n$ 的 n 个方程组成的齐次线性方程组

$$\begin{cases}\sigma_0(\alpha_1)x_0+\sigma_1(\alpha_1)x_1+\cdots+\sigma_n(\alpha_1)x_n=0\\ \cdots \qquad \cdots \qquad \cdots \qquad \cdots\\ \sigma_0(\alpha_n)x_0+\sigma_1(\alpha_n)x_1+\cdots+\sigma_n(\alpha_n)x_n=0\end{cases}$$

必有非零解,取一个非零解 $(c_0,c_1,\cdots,c_n)\in E'^{n+1}$.由于 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 E/F 的一个基,因此对于任意 $\alpha\in E$,有

$$\alpha=\sum_{j=1}^{n}a_j\alpha_j,\quad a_j\in F,\quad j=1,2,\cdots,n$$

于是

$$\sum_{i=0}^{n}c_i\sigma_i(\alpha)=\sum_{i=0}^{n}c_i\sigma_i\Big(\sum_{j=1}^{n}a_j\alpha_j\Big)=\sum_{i=0}^{n}c_i\sum_{j=1}^{n}a_j\sigma_i(\alpha_j)$$

$$=\sum_{j=1}^{n}\Big(\sum_{i=0}^{n}c_i\sigma_i(\alpha_j)\Big)a_j=\sum_{j=1}^{n}0a_j=0,$$

从而 $\sum_{i=0}^{n}c_i\sigma_i=0$.因此 $\sigma_0,\sigma_1,\cdots,\sigma_n$ 在 E' 上线性相关.这与引理 1 矛盾.因此存在至多 n 个从 E 到 E' 的 F - 同态. □

注:设 $[E:F]<\infty$,则当 $E=E'$ 时,域 E 到 E 的任一 F - 同态必定是 F - 同构.理由如下:设 σ 是域 E 到自身的一个同态,则 $\operatorname{Ker}\sigma$ 是 E 的理想.从而 $\operatorname{Ker}\sigma=(0)$ 或 $\operatorname{Ker}\sigma=E$.后者表明 $\sigma=0$,这与 σ 是环同态矛盾.因此 $\operatorname{Ker}\sigma=(0)$.从而 σ 是单射.由于 σ 是域 E 到 E 的 F - 同态,因此 σ 是域 F 上线性空间 E 上的一个线性变换,又由于 $\dim_F E=[E:F]<\infty$,因此从 σ 是单射可推出 σ 是满射,从而 σ 是域 E 到 E 的 F - 同构.

定理 2(Artin) 设 E 是一个域，G 是 E 的一个自同构群. 令

$$K = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\},$$

则 (1) K 是 E 的一个子域，称 K 是 G 的**不动域**(fixed field) 记作 $\mathrm{Inv}(G)$.

(2) $[E:K]$ 有限当且仅当 G 是有限群，此时

$$[E:K] = |G|.$$

证明 (1) 设 $k_1, k_2 \in K$，任取 $\sigma \in G$，有

$$\sigma(k_1 - k_2) = \sigma(k_1) - \sigma(k_2) = k_1 - k_2,$$

$$\sigma(k_1 k_2^{-1}) = \sigma(k_1)\sigma(k_2)^{-1} = k_1 k_2^{-1},$$

因此 $k_1 - k_2, k_1 k_2^{-1} \in K$，从而 K 是 E 的一个子域.

(2) 必要性. 设 $[E:K] = n$. 据定理 1 和注得，存在至多 n 个 E 的 K－自同构，从而 $|G| \leqslant n = [E:K]$. 下面来证等号成立. 设 $|G| = r$，且设 $G = \{\sigma_1, \cdots, \sigma_r\}$. 假如 $r < [E:K]$，则 $[E:K] \geqslant r+1$. 从而在 E 中存在 $r+1$ 个元素 $\alpha_0, \alpha_1, \cdots, \alpha_r$ 在 K 上线性无关. 任取 $\sigma \in G$，域 E 上 $r+1$ 个未知量 $x_0, x_1, x_2, \cdots, x_r$ 的齐次线性方程组

$$\begin{cases} \sum_{i=0}^{r} \sigma_1(\alpha_i) x_i = 0 \\ \cdots\cdots \\ \sum_{i=0}^{r} \sigma_r(\alpha_i) x_i = 0 \end{cases} \tag{6}$$

必有非零解. 取一个非零解 $(c_0, c_1, \cdots, c_r) \in E^{r+1}$，且它具有最少的非零元. 不妨设 $c_0 \neq 0$. 则从

$$\sum_{i=0}^{r} \sigma_j(\alpha_i) c_i = 0$$

可解出

$$\sigma_j(\alpha_0) = \sum_{i=1}^{r} \sigma_j(\alpha_i) b_i, \tag{7}$$

其中 $b_i = -\frac{c_i}{c_0}$，$1 \leqslant i \leqslant r$，$1 \leqslant j \leqslant r$. G 中的单位元设为 σ_1. 由上式

得

$$\alpha_0 = \sigma_1(\alpha_0) = \sum_{i=1}^{r} \sigma_1(\alpha_i) b_i = \sum_{i=1}^{r} \alpha_i b_i.$$

由于 $\alpha_0, \alpha_1, \cdots, \alpha_r$ 在 K 上线性无关，因此 $b_1, \cdots, b_r$ 不能全属于 K. 不妨设 $b_1 \notin K$. 于是存在 $\sigma_l \in G$ 使得 $\sigma_l(b_1) \neq b_1$. (7) 式中 σ_j 换成 $\sigma_l^{-1}\sigma_j$，得

$$\sigma_l^{-1}\sigma_j(\alpha_0) = \sum_{i=1}^{r} \sigma_l^{-1}\sigma_j(\alpha_i) b_i, \quad j = 1,2,\cdots,r.$$

两边用 σ_l 作用得

$$\sigma_j(\alpha_0) = \sum_{i=1}^{r} \sigma_j(\alpha_i)\sigma_l(b_i), \quad j = 1,2,\cdots,r. \tag{8}$$

(7) − (8)，得

$$0 = \sum_{i=1}^{r} \sigma_j(\alpha_i)[b_i - \sigma_l(b_i)]. \tag{9}$$

于是 r 元齐次线性方程组

$$0 = \sum_{i=1}^{r} \sigma_j(\alpha_i) y_i, \quad j = 1,2,\cdots,r. \tag{10}$$

有非零解 $(b_1 - \sigma_l(b_1), \cdots, b_r - \sigma_l(b_r))$. 在最前面添上一个分量 0，则得到方程组 (6) 的一个非零解. 把 $(c_0, c_1, \cdots, c_r)$ 与 $(0, b_1 - \tau(b_1), \cdots, b_r - \tau(b_r))$ 比较，当 $c_i = 0$ 时，有 $b_i = -\dfrac{c_i}{c_0} = 0$. 从而必有 $b_i - \sigma_l(b_i) = 0$；而 $c_i \neq 0$ 时，有 $b_i - \sigma_l(b_i) = -\dfrac{c_i}{c_0} - \sigma_l\left(-\dfrac{c_i}{c_0}\right)$，它可能为 0，也可能不为 0. 又由于 $c_0 \neq 0$，因此 $(0, b_1 - \sigma_l(b_1), \cdots, b_r - \sigma_l(b_r))$ 的非零分量数目少于 $(c_0, c_1, \cdots, c_r)$ 的非零分量数目. 这与 $(c_0, c_1, \cdots, c_r)$ 的取法矛盾. 所以 $r = [E:K]$，即 $|G| = [E:K]$.

充分性. 设 $|G| = r$. 假如 $[E:K] > r$，则 E 中存在 $r+1$ 个元素 $\alpha_0, \alpha_1, \cdots, \alpha_r$ 在 K 上线性无关. 由刚才的推导过程得出矛盾. 因此 $[E:K] = r$. ∎

推论 3　设 E/K 是有限扩张，G 是 E 的所有 K－自同构组成的集合，它是一个群．如果 E 中 G 的不动域等于 K，则 $|G|=[E:K]$．

证明　从定理 2 的必要性立即得到．　□

从推论 3 受到启发，引进下述概念．

定义 1　设 E/F 为任一域扩张，E 的所有 F－自同构成一群，称它为 E/F 的**伽罗瓦群**(Galois group)．记作 $\mathrm{Gal}(E/F)$．

定义 2　如果域扩张 E/F 的伽罗瓦群 $\mathrm{Gal}(E/F)$ 的不动域等于 F，则 E/F 称为一个**伽罗瓦扩张**(Galois extension)．

从推论 3 立即得出：

推论 4　如果有限扩张 E/F 是伽罗瓦扩张，则它的伽罗瓦群 $\mathrm{Gal}(E/F)$ 的阶等于扩张次数 $[E:F]$．　□

下面我们介绍著名的伽罗瓦基本定理．

伽罗瓦基本定理　设 E/F 为一个有限伽罗瓦扩张，$G=\mathrm{Gal}(E/F)$，则

(i) 在 G 的子群集 $\{H\}$ 和 E/F 的中间域集 $\{K\}$ 之间存在一个一一对应．让每个子群 H 对应于它的不动域：

$$H\longmapsto \mathrm{Inv}(H),$$

让每个中间域 K 对应于 E 对 K 的伽罗瓦群：

$$K\longmapsto \mathrm{Gal}(E/K).$$

于是它们互为逆映射，即

$$\mathrm{Gal}(E/\mathrm{Inv}(H))=H,$$
$$\mathrm{Inv}(\mathrm{Gal}(E/K))=K.$$

(ii) 上述一一对应是反包含的，即

$$H_1\subseteq H_2 \Longleftrightarrow \mathrm{Inv}(H_1)\supseteq Inv(H_2).$$

(iii) 有数量关系：

$$[E:\mathrm{Inv}(H)]=|H|,$$
$$[\mathrm{Inv}(H):F]=[G:H].$$

(iv) 若子群 H 对应于中间域 K，则 H 的共轭子群 $\sigma H\sigma^{-1}$ 对应于 K 的共轭子域 $\sigma(K)$，$\sigma \in G$.

(v) 设子群 H 对应于中间域 K，则 H 是 G 的正规子群当且仅当 K/F 上是伽罗瓦扩张.

证明可看聂灵沼、丁石孙著《代数学引论(第二版)》第 243 – 244 页.

历史上对于伽罗瓦扩张有另一种定义：域扩张 E/F 称为伽罗瓦扩张，如果 E 是 F 上一个无重根的多项式的分裂域. 这个定义与上面的定义 2 是等价的，即

定理 5 一个有限扩张 E/F 是伽罗瓦扩张当且仅当 E/F 是一个可分正规扩张. 或者说，一个有限扩张 E/F 是伽罗瓦扩张当且仅当 E 是 F 上一个可分多项式(即无重根的多项式)的分裂域.

证明 定理 5 中第一个结论的证明可看聂灵沼、丁石孙著《代数学引论(第二版)》第 245 页，然后结合本章 §1 的定理 9 便得到定理 5 中的第二个结论.

在一些具体问题中，利用定理 5 的第二句话，常常比较容易判断一个有限扩张 E/F 是伽罗瓦扩张.

在证明上述定理 5 的第一句话的必要性时，主要用到下面的引理 2，而引理 2 本身也是很有用的.

引理 2 设 E/F 是一个有限伽罗瓦扩张，G 是它的伽罗瓦群. 则 E 的任一元素 α 在 F 上的极小多项式 $m(x)$ 是可分的(即没有重根)，而且 $m(x)$ 的全部根组成的集合恰好是 α 在 G 作用下得到的所有像组成的集合(即，α 的 G – 轨道).

证明 设 $\Omega = \{\alpha_1, \alpha_2, \cdots, \alpha_r\}$ 是 α 在 G 作用下得到的所有像组成的集合(作为集合的元素，$\alpha_1, \alpha_2, \cdots, \alpha_r$ 两两不同)，其中 $\alpha_1 = \alpha$. 令

$$g(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_r).$$

对于任一 $\sigma \in G$，由 Ω 的定义知道，$\sigma(\alpha_1), \sigma(\alpha_2), \cdots, \sigma(\alpha_r)$ 是 α_1,

$\alpha_2, \cdots, \alpha_r$ 的一个排列. 因此 $g(x)$ 的系数在 σ 作用下不变. 于是 $g(x)$ 是 $F[x]$ 中的一个多项式. 下面证明 $g(x)$ 在 F 上不可约. 设 $f(x)$ 是 $F[x]$ 中以 α 为根的任一多项式, $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$. 用 σ 作用于 $f(\alpha) = 0$, 得

$$\sigma(\alpha)^n + a_1\sigma(\alpha)^{n-1} + \cdots + a_{n-1}\sigma(\alpha) + a_n = 0.$$

因此 $\sigma(\alpha)$ 也是 $f(x)$ 的根, $\forall \sigma \in G$. 即每个 α_i 都是 $f(x)$ 的根, $i = 1,2,\cdots,r$. 从而 $g(x) \mid f(x)$. 于是 $g(x)$ 在 $F[x]$ 中的因式只有 F 中的非零元和 $g(x)$ 的相伴元. 因此 $g(x)$ 在 F 上不可约. 在 F 上以 α 为根的首项系数为 1 的不可约多项式是唯一的, 因此 $g(x) = m(x)$. 这证明了 $m(x)$ 是可分的, 并且 $m(x)$ 的全部根组成的集合恰好是 α 在 G 作用下得到的所有像组成的集合 $\{\alpha_1, \alpha_2, \cdots, \alpha_r\}$. □

定义 3 设 E/F 是一个有限伽罗瓦扩张, E 中两个元素 α 与 β 称为**共轭的**(conjugate), 如果它们属于同一条 $\mathrm{Gal}(E/F)$－轨道.

由引理 2 立即得到.

推论 6 有限伽罗瓦扩张 E/F 的两个元素是共轭的当且仅当它们在 F 上的极小多项式相同. □

设 $f(x)$ 是域 F 上一个无重根的 n 次($n \geq 1$) 多项式, 设 E 是 $f(x)$ 在 F 上的分裂域. 于是 $E = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$, α_i 为 $f(x)$ 的根, $1 \leq i \leq n$. 据定理 5 得, E/F 是有限伽罗瓦扩张, 再据引理 2 可得, E/F 的伽罗瓦群 G 的任一元素 σ 引起 $f(x)$ 的全部根组成的集合 Ω 上的一个置换 π_σ. 而且显然对于 $\sigma, \tau \in G$, 有 $\pi_\sigma\pi_\tau = \pi_{\sigma\tau}$; 当 $\sigma \neq \tau$, 则 $\pi_\sigma \neq \pi_\tau$. 于是我们得到 G 到 S_Ω 的一个单同态 $\psi: \sigma \mapsto \pi_\sigma$, 从而 $\mathrm{Im}\psi \cong G$. 我们把 $\mathrm{Im}\psi$ 记作 G_f.

定义 4 设 $f(x)$ 是域 F 上一个无重根的 $n(n \geq 1)$ 次多项式, E 是 $f(x)$ 在 F 上的分裂域, 则上述 G_f 称为 $f(x)$ 在 F 上的**伽罗瓦群**, 或简称为 $f(x)$ 在 F 上的群.

从上面的讨论知道, $f(x)$ 在 F 上的伽罗瓦群 G_f 是 $f(x)$ 在它的

分裂域 E 中的全部根组成的集合 Ω 上的置换群，并且 G_f 与 E/F 的伽罗瓦群 $\mathrm{Gal}(E/F)$ 同构.

如果 G_f 在 Ω 上是传递的，则 $f(x)$ 的根 $\alpha_1,\cdots,\alpha_n$ 在 G_f 下组成一个传递集. 从引理 2 的证明过程看到，$f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ 在 F 上不可约. 反之，设 $f(x)$ 不可约，仍据引理 2，含有 α_1 的传递集恰好是 α_1 的极小多项式 $f(x)$ 的全部根，因而 $\{\alpha_1,\cdots,\alpha_n\}$ 是在 G_f 下含 α_1 的传递集. 这表明 G_f 在 Ω 上是传递的，我们把这个结论写成命题 7.

命题 7 设 $f(x)$ 是域 F 上一个无重根的 $n(n\geqslant 1)$ 次多项式，则 $f(x)$ 在 F 上的伽罗瓦群 G_f 是传递的当且仅当 $f(x)$ 在 F 上不可约. □

现在我们来决定有限域的伽罗瓦群.

定理 8 设 $q=p^n$，p 为素数. 令

$$\sigma_p: F_q \longrightarrow F_q$$
$$\alpha \longmapsto \alpha^p,$$

则 $\mathrm{Gal}(F_q/F_p)=\langle\sigma_p\rangle$，它是 n 阶循环群.

证明 从本章 §1 的定理 7 的证明中看到，F_q 是域 F_p 上的多项式 x^q-x 在 F_p 上的分裂域，并且 x^q-x 无重根. 据定理 5 得，F_q/F_p 是伽罗瓦扩张. 据推论 4 得，伽罗瓦群 $\mathrm{Gal}(F_q/F_p)$ 的阶等于扩张次数 $[F_q:F_p]=n$.

对于任意 $\alpha,\beta\in F_q$，有

$$\sigma_p(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\beta^p=\sigma_p(\alpha)+\sigma_p(\beta),$$
$$\sigma_p(\alpha\beta)=(\alpha\beta)^p=\alpha^p\beta^p=\sigma_p(\alpha)\sigma_p(\beta).$$

因此 σ_p 是环同态. 任取 $\gamma\in\mathrm{Ker}\sigma_p$，则 $\sigma_p(\gamma)=0$，于是 $\gamma^p=0$. 由此推出 $\gamma=0$. 因此 $\mathrm{Ker}\sigma_p=\{0\}$. 从而 σ_p 是单射. 由于 F_q 是有限集，因此 σ_p 也是满射. 从而 σ_p 是域 F_q 的一个自同构. 对于任意 $a\in F_p$，有 $\sigma(a)=a^p=a$. 因此 σ_p 是一个 F_p-自同构. 从而 $\sigma_p\in$

$\mathrm{Gal}(F_q/F_p)$.

对于任意 $\alpha \in F_q$，有

$$\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha^q = \alpha.$$

因此 σ_p^n 是 F_q 的恒等变换. F_q^* 是 $q-1$ 阶循环群，设 ξ 是 F_q^* 的生成元，则当 $l < n$ 时，有

$$\sigma_p^l(\xi) = \xi^{p^l} \neq \xi,$$

从而 $\langle \sigma_p \rangle$ 的阶为 n. 因此 $\mathrm{Gal}(F_q/F_p) = \langle \sigma_p \rangle$. □

定理 8 中的 σ_p 称为有限域 F_q 的 Frobenius **自同构**(Frobenius automorphism).

定理 9　设 $q = p^n$，p 为素数. 令

$$\sigma_q : F_{q^m} \longrightarrow F_{q^m}$$
$$\alpha \longmapsto \alpha^q,$$

则 $\mathrm{Gal}(F_{q^m}/F_q) = \langle \sigma_q \rangle$，它是 m 阶循环群.

证明　类似于本章 §1 的定理 7 的证明可知，域 F_q 上的多项式 $x^{q^m} - x$ 无重根. 由于域 F_q 与它的子域 F_p 的单位元是同一个元素，因此 $x^{q^m} - x$ 也可看成是 F_p 上的多项式 $x^{p^{mn}} - x$，而后者在 F_p 上的分裂域是 $F_{p^{mn}} = F_{q^m}$. 从而 $x^{q^m} - x$ 在 F_q 上的分裂域是 F_{q^m}. 于是 F_{q^m}/F_q 是伽罗瓦扩张. 从而

$$|\mathrm{Gal}(F_{q^m}/F_q)| = [F_{q^m} : F_q] = m.$$

容易验证，σ_q 是环同态，且 σ_q 是单射，从而也是满射，因此 σ_q 是域 F_{q^m} 的一个自同构. 易知 σ_q 是 F_q - 自同构. 从而 $\sigma_q \in \mathrm{Gal}(F_{q^m}/F_q)$. 容易证明，$\langle \sigma_q \rangle$ 的阶为 m. 因此 $\mathrm{Gal}(F_{q^m}/F_q) = \langle \sigma_q \rangle$. □

习题 3.2

1. 设 $f(x) = x^3 - 2 \in \mathbf{Q}[x]$,

(1) 求 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域 E;(2) 求 $\mathrm{Gal}(E/\mathbf{Q})$.

2. 求有限域 F_{2^m} 的伽罗瓦群 $\mathrm{Gal}(F_{2^m}/F_2)$.

§3 本原元素,迹与范数

一个有限扩张如果是单扩张,那是我们特别感兴趣的.

定义 1 设 K/F 是一个有限扩张,如果 $K = F(\alpha)$,则称 α 是 K/F 的一个**本原元素**(primitive element).

设 $q = p^n$, p 为素数.有限域 F_q 的非零元素组成的乘法群 F_q^* 是循环群,设 α 为 F_q^* 的一个生成元,则显然有 $F_q = F_p(\alpha)$.于是 α 为 F_q/F_p 的一个本原元素.但是 F_q/F_p 的一个本原元素不一定是 F_q^* 的生成元,例如,$F_{25} = F_5[x]/(x^2+x+1) = F_5(u)$,其中 $u = x + (x^2+x+1)$.因此 u 是 F_{25}/F_5 的一个本原元素.但是由于 $u^2+u+1=0$,因此 $u^3 = u(4u+4) = 4u^2+4u = 4(4u+4)+4u = 1$.从而 u 是 F_{25}^* 的 3 阶元.于是 u 不是 F_{25}^* 的生成元.

考虑任一有限域 F_q 上的有限扩张 F_{q^m}/F_q.与上述讨论一样,由于 $F_{q^m}^*$ 是循环群,设它的一个生成元为 ξ,则 $F_{q^m} = F_q(\xi)$.从而 ξ 是 F_{q^m}/F_q 的一个本原元素.但是 F_{q^m}/F_q 的一个本原元素不一定是 $F_{q^m}^*$ 的生成元.

从上述讨论看出,有限域上的有限扩张都是单扩张.

下面我们来介绍两个重要的概念:迹和范数.

定义 2 设 E/F 为一个有限伽罗瓦扩张,$G = \mathrm{Gal}(E/F)$.对于任一 $\alpha \in E$,令

$$\mathrm{Tr}_{E/F}(\alpha) \xlongequal{\text{def}} \sum_{\sigma \in G} \sigma(\alpha), \tag{1}$$

$$\mathrm{N}_{E/F}(\alpha) \xlongequal{\text{def}} \prod_{\sigma \in G} \sigma(\alpha), \tag{2}$$

则称 $\mathrm{Tr}_{E/F}(\alpha)$ 是 α 的**迹**(trace),称 $\mathrm{N}_{E/F}(\alpha)$ 是 α 的**范数**(norm).在不至于引起含混的情况下,它们可分别记作 $\mathrm{Tr}(\alpha)$ 和 $\mathrm{N}(\alpha)$.

自然要问 $\mathrm{Tr}(\alpha)$ 和 $\mathrm{N}(\alpha)$ 属于哪个域?任意给定 $\alpha\in E$,设 α 在 F 上的极小多项式为 $m(x)$,它的次数为 r.由于 E/F 是有限伽罗瓦扩张,因此根据本章 §2 的引理 2 得,$m(x)$ 没有重根,而且 $m(x)$ 的全部根组成的集合恰好是 α 的 G–轨道 $G(\alpha)$.由于 $m(x)$ 的全部根的和等于 $m(x)$ 的 $r-1$ 次项的系数的相反数,因此 $\mathrm{Tr}(\alpha)=\sum\limits_{\sigma\in G}\sigma(\alpha)\in F$.又由于 $m(x)$ 的全部根的积等于 $m(x)$ 的常数项乘以 $(-1)^r$,因此 $\mathrm{N}(\alpha)=\prod\limits_{\sigma\in G}\sigma(\alpha)\in F$.这表明 Tr 和 N 都是 E 到 F 的映射.这正是它们的威力之所在:把 E 中的元素"变"成 F 的元素.不仅如此,它们还有很好的性质.

命题 1　设 E/F 为一个有限伽罗瓦扩张,$[E:F]=n$,$G=\mathrm{Gal}(E/F)$.则对于任意 $\alpha,\beta\in E$、$a\in F$,有

(1) $\mathrm{Tr}(\alpha+\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta)$;

(2) $\mathrm{Tr}(a\alpha)=a\mathrm{Tr}(\alpha)$;

(3) $\mathrm{Tr}(a)=na$;

(4) $\mathrm{N}(\alpha\beta)=\mathrm{N}(\alpha)\mathrm{N}(\beta)$;

(5) $\mathrm{N}(a\alpha)=a^n\mathrm{N}(\alpha)$;

(6) $\mathrm{N}(a)=a^n$.

证明　(1)
$$\mathrm{Tr}(\alpha+\beta)=\sum_{\sigma\in G}\sigma(\alpha+\beta)=\sum_{\sigma\in G}[\sigma(\alpha)+\sigma(\beta)]=\sum_{\sigma\in G}\sigma(\alpha)+\sum_{\sigma\in G}\sigma(\beta)=\mathrm{Tr}(\alpha)+\mathrm{Tr}(\beta).$$

(2)
$$\mathrm{Tr}(a\alpha)=\sum_{\sigma\in G}\sigma(a\alpha)=\sum_{\sigma\in G}\sigma(a)\sigma(\alpha)=\sum_{\sigma\in G}a\sigma(\alpha)=a\mathrm{Tr}(\alpha).$$

(3)～(6) 可以类似地证明.　□

从命题 1 的(1)和(2)看到,Tr 是域 F 上线性空间 E 上的一个线

性函数，称它为迹函数. 令

$$f(\alpha,\beta)\xlongequal{\text{def}}\mathrm{Tr}(\alpha\beta),\quad\forall\alpha,\beta\in E.\tag{3}$$

显然 f 是 E 上的对称双线性函数.

定理 2 设 E/F 为一个有限伽罗瓦扩张，$[E:F]=n$，$G=\mathrm{Gal}(E/F)$，则利用迹函数定义的对称双线性函数 f 是非退化的.

证明 取 E 的一个基 $\alpha_1,\alpha_2,\cdots,\alpha_n$，由于 $[E:F]=n$，因此 $|G|=[E:F]=n$，设 $G=\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$.

$f(\alpha,\beta)$ 在基 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 下的度量矩阵 A 的 (i,j) 元为

$$f(\alpha_i,\alpha_j)=\mathrm{Tr}(\alpha_i\alpha_j)=\sum_{l=1}^{n}\sigma_l(\alpha_i\alpha_j)=\sum_{l=1}^{n}\sigma_l(\alpha_i)\sigma_l(\alpha_j).$$

令 n 级矩阵 D 的 (i,l) 元为 $\sigma_l(\alpha_i)$，则

$$\begin{aligned}A(i;j)&=\sum_{l=1}^{n}\sigma_l(\alpha_i)\sigma_l(\alpha_j)=\sum_{l=1}^{n}D(i;l)D(j;l)\\&=\sum_{l=1}^{n}D(i;l)D'(l;j)=(DD')(i;j).\end{aligned}$$

由此得出，$A=DD'$.

根据本章 §2 的引理 1（Dedekind 引理），$\sigma_1,\sigma_2,\cdots,\sigma_n$ 在域 E 上是线性无关的. 考虑域 E 上的线性方程组

$$DX=0.\tag{4}$$

假如 D 不可逆，则方程组(4) 有非零解 $(c_1,c_2,\cdots,c_n)'$. 于是

$$c_1\begin{pmatrix}\sigma_1(\alpha_1)\\\sigma_1(\alpha_2)\\\vdots\\\sigma_1(\alpha_n)\end{pmatrix}+c_2\begin{pmatrix}\sigma_2(\alpha_1)\\\sigma_2(\alpha_2)\\\vdots\\\sigma_2(\alpha_n)\end{pmatrix}+\cdots+c_n\begin{pmatrix}\sigma_n(\alpha_1)\\\sigma_n(\alpha_2)\\\vdots\\\sigma_n(\alpha_n)\end{pmatrix}=0.\tag{5}$$

任取 $\beta\in E$，设 $\beta=\sum_{j=1}^{n}b_j\alpha_j$，$b_j\in F$，$j=1,2,\cdots,n$，则

$$\Big(\sum_{i=1}^{n}c_i\sigma_i\Big)\beta=\sum_{i=1}^{n}c_i\sigma_i(\beta)=\sum_{i=1}^{n}c_i\sigma_i\Big(\sum_{j=1}^{n}b_j\alpha_j\Big)$$

$$\sum_{j=1}^{n} b_j\left(\sum_{i=1}^{n} c_i\sigma_i(\alpha_j)\right) = \sum_{j=1}^{n} b_j 0 = 0.$$

由此推出，$\sum_{i=1}^{n} c_i\sigma_i = 0$. 这表明 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 在 E 上线性相关. 矛盾. 因此 D 可逆. 从而 A 也可逆，于是 f 是非退化的. □

推论 3 设 E/F 为一个有限伽罗瓦扩张，$[E:F] = n$. 则迹函数 Tr 是满射.

证明 由于用迹函数定义的对称双线性函数 $f(\alpha, \beta)$ 是非退化的，因此 $\mathrm{Tr} \neq 0$. 从而 $\mathrm{Im Tr} \neq 0$. 由于 ImTr 是域 F 上线性空间 F 的子空间，而 $\dim_F F = 1$，且 $\dim_F(\mathrm{ImTr}) \neq 0$. 因此 $\dim_F(\mathrm{ImTr}) = 1$. 从而 $\mathrm{ImTr} = F$. 这表明迹函数 Tr 是满射. □

现在设 $F = GF(q)$，q 是素数 p 的方幂，$E = GF(q^m)$. 从本章§2的定理9知道，$GF(q^m)/GF(q)$ 是伽罗瓦扩张，并且它的伽罗瓦群 $G = \langle\sigma_q\rangle$，它是 m 阶循环群. 据定义2得，对于任一 $\alpha \in GF(q^m)$，有

$$\mathrm{Tr}_{E/F}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{m-1}}, \tag{6}$$

$$\mathrm{N}_{E/F}(\alpha) = \alpha\alpha^q\alpha^{q^2}\cdots\alpha^{q^{m-1}} = \alpha^{\frac{q^m-1}{q-1}}. \tag{7}$$

如果取 $F = F_p$，$E = F_{p^r}$，则对于 $\alpha \in F_{p^r}$，有

$$\mathrm{Tr}_{F_{p^r}/F_p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{r-1}}. \tag{8}$$

今后我们把 F_{p^r}/F_p 的迹函数称为有限域的**绝对迹函数**，就记作 Tr. 把 F_{q^m}/F_q 的迹函数 $\mathrm{Tr}_{F_{q^m}/F_q}$ 称为**相对迹函数**.

定理 4(传递公式) 设 E/F 是一个有限伽罗瓦扩张，L 是一个中间域，即 $E \supseteq L \supseteq F$. 则对于任一 $\alpha \in E$，有

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}_{L/F}(\mathrm{Tr}_{E/L}(\alpha)), \tag{9}$$

$$\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{L/F}(\mathrm{N}_{E/L}(\alpha)). \tag{10}$$

证明可看 P. M. Cohn 著《Algebra, vol. 2 (Second Edition)》

习题 3.3

1. 找出 $GF(27)/GF(3)$ 的一个本原元素.

2. 证明:对于任一 $\alpha \in GF(2^m)/GF(2)$,有

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2).$$

3. 设 G 是有限域 $GF(q)$ 的加法群, $q = p^n$, p 为素数. 设 ξ 是复数域中的一个本原 p 次单位根. 任意取定一个 $a \in GF(q)$, 令

$$\begin{aligned} \chi_a : G &\longrightarrow \mathbf{C}^* \\ x &\longmapsto \xi^{\mathrm{Tr}(ax)}, \end{aligned} \tag{11}$$

其中 Tr 是 $GF(q)/GF(p)$ 的迹函数(把 $GF(p)$ 看成 $\mathbf{Z}_p$).

证明:(1) χ_a 是加法群 G 到乘法群 $\mathbf{C}^*$ 的一个同态;

(2) 如果 $a, b \in GF(q)$, 且 $a \neq b$, 则

$$\chi_a \neq \chi_b.$$

(注:对于 $\bar{i} \in \mathbf{Z}_p$, 定义 $\xi^{\bar{i}} = \xi^i$. 容易看出这个定义是合理的.)

习题的提示或答案

引言的习题

1. 假如 $ax=b$ 有解，两边左乘 a^{-1}，得 $x=a^{-1}b$；把 x 用 $a^{-1}b$ 代入，原方程左端为 $a(a^{-1}b)=b$，与右端相等. 从而 $x=a^{-1}b$ 是 $ax=b$ 的解，并且它是唯一的解.

$ya=b$ 有唯一解的证法类似.

2. 等式两边左乘 a^{-1}（或右乘 a^{-1}）即得.

3. 否. 因为 $\bar{2}$ 不是可逆元.

4. $\bar{1},\bar{3},\bar{5},\bar{7}$.

*5. 利用 $(a,m)=1$ 当且仅当存在 $u,v\in\mathbf{Z}$，使得 $ua+vm=1$.

第一章　群

习题 1.1

1. 用 σ 表示绕顶点与底面中心连线转角为 $\frac{\pi}{6}$ 的旋转. 则正十二棱锥的旋转对称(性)群 G 为

$$G=\{\sigma^k \mid k=0,1,2,\cdots,11\}.$$

G 是循环群.

2. $D_6=\{I,\sigma,\sigma^2,\cdots\sigma^5,\tau_1,\tau_2,\cdots\tau_6\}$，

其中 σ 是绕正六边形中心转角为 $\frac{\pi}{3}$ 的旋转，$\tau_1,\cdots,\tau_6$ 是关于每一条

对称轴的反射,共有6条对称轴:3条主对角线,3条对边中点连线.σ、τ_1是D_6的生成元,它们适合的关系有$\sigma^6=I$,$\tau_1^2=I$,$\tau_1\sigma\tau_1=\sigma^{-1}$,$|D_6|=12$.

3. 画出图形,说出$\sigma^j\tau$表示关于哪一条对称轴的反射($j=1,2,3,4$).经计算得,$(\sigma\tau)(\sigma^2\tau)=\sigma^4$.

4. 用σ_i表示绕一个顶点与对面中心连线转角为$\frac{2\pi}{3}$的旋转,$i=1,2,3,4$;用γ_j表示绕对棱中点连线转角为π的旋转,$j=1,2,3$.则正四面体的旋转对称(性)群G满足$G\supseteq\{I,\sigma_i,\sigma_i^2,\gamma_j\mid 1\leqslant i\leqslant 4,1\leqslant j\leqslant 3\}$.

用A_i表示正四面体的顶点,并且使$A_1A_2A_3A_4$成右手螺旋方向.则G中任一元素γ使$A_1A_2A_3A_4$或者仍成右手螺旋方向,或者成左手螺旋方向.由此去证γ或者为某个σ_i或σ_i^2,或者为某个γ_j.从而G恰好由上述12个元素组成.

*5. 用r_i表示绕正方体对面中心连线转角为$\frac{\pi}{2}$的旋转,$i=1,2,3$;用s_j表示绕主对角线转角为$\frac{2\pi}{3}$的旋转,$j=1,2,3,4$;用t_k表示绕对棱中点连线转角为π的旋转,$k=1,2,3,4,5,6$.则正方体的旋转对称(性)群G满足$G\supseteq\{I,r_i,r_i^2,r_i^3,s_j,s_j^2,t_k\mid 1\leqslant i\leqslant 3,1\leqslant j\leqslant 4,1\leqslant k\leqslant 6\}$.类似于第4题的方法可证$G$恰好由这24个元素组成.

6. $U(\mathbf{Z}_{15})=\{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\}$,阶为8.

*7. 由引言的习题第5题的结论即得.

8. (1) 计算AA'和$|A|$;

(2) A表示的旋转$\mathbf{A}$保持顶点O不动,再找出$\mathbf{A}$的一个不动点M,则OM就是$\mathbf{A}$的转轴.设点M的坐标为$X=(x_1,x_2,x_3)'$.则$\mathbf{A}X=X$.即$AX=X$.即$(I-A)X=0$.由此解出一个基础解系为$(1,-1,1)'$.于是点M的坐标为$(1,-1,1)'$.

9.(1) $\sigma_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}, \sigma_2\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$.

(2) $\sigma_1 = (13542)$, $\sigma_2 = (143)(25)$.

(3) $\sigma_1^{-1} = (12453)$, $\sigma_1\sigma_2\sigma_1^{-1} = (325)(14)$.

(4) $\sigma_1 = (12)(14)(15)(13)$; $\sigma_2 = (13)(14)(25)$.

(5) σ_1 是偶置换，σ_2 是奇置换.

10. 因为 $(i_1 i_2 i_3 \cdots i_{r-1} i_r) = (i_1 i_r)(i_1 i_{r-1})\cdots(i_1 i_3)(i_1 i_2)$，所以 r－轮换为偶置换当且仅当 r 为奇数.

11. $A_3 = \{(1),(123),(132)\}$;
$A_4 = \{(1),(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),(234),(243)\}$.

12. 任取 $k \in \{1,2,\cdots,r-1\}$，去计算 $(\tau\sigma\tau^{-1})[\tau(i_k)]$；此外去计算 $(\tau\sigma\tau^{-1})[\tau(i_r)]$.

任取 $a \in \Omega \setminus \{\tau(i_1),\cdots\tau(i_r)\}$，去计算 $(\tau\sigma\tau^{-1})(a)$.

习题 1.2

1.(1) 去证 $km - kl \in k\mathbf{Z}$，又显然 $0 \in k\mathbf{Z}$.

(2) $km = mk$，从而 $k\mathbf{Z} = \langle k \rangle$.

2. 必要性. 任取 $hk \in HK$，设 hk 的逆为 h_1k_1，去证 $hk \in KH$，从而 $HK \subseteq KH$，同理 $KH \subseteq HK$.

充分性. 任取 $h_1k_1, h_2k_2 \in HK$，去证 $(h_1k_1)(h_2k_2)^{-1} \in HK$，注意利用条件 $HK = KH$.

3. $\langle 1, i \rangle = \{m + ni \mid m, n \in \mathbf{Z}\}$.

4. 棋盘的对称(性)群 $G = \{I, \sigma^2, \tau_1, \tau_2\}$，其中 σ 是绕正方形的中心转角为 $\frac{\pi}{2}$ 的旋转，τ_i 是关于对角线的反射，$i = 1,2$.

*5. 我们已证 $S_n = \langle (12),(13),\cdots,(1n) \rangle$. 因此只要对于 $k \in \{3,4,\cdots,n\}$，去证 $(1k)$ 可以表示成 $(12),(23),\cdots,(n-1,n)$ 这些

对换的乘积(它们可重复出现),例如,$(13) = (23)(12)(23)$,这里利用了习题 1.1 的第 12 题的结论.

(2) 据第(1)小题的结论,只要去证$(k\ \ k+1)$可以表示成(12),$(123\cdots n)^j$的乘积(可重复出现),$-n < j < n$.注意利用习题 1.1 的第 12 题的结论,例如

$(23) = (123\cdots n)(12)(123\cdots n)^{-1}$,

$(34) = (123\cdots n)(23)(123\cdots n)^{-1}$,

…….

6.(1) 由于 $S_n = \langle (12),(13),\cdots(1n)\rangle$,且偶置换可表示成偶数个对换的乘积,因此只要考察$(1i)(1j)$.

*(2) 只在去证任一 3 - 轮换$(ijk) \in \langle (123),(124),\cdots,(12n)\rangle$.注意利用习题 1.1 的第 12 题的结论.

7. 计算 $A^2, A^3, A^4; B^2, B^3; (AB)^m$.

8. G 中任取两个非单位元a, b.去证 $ab = ba$.注意 2 阶元的逆是它自身.

*9. 用反证法.假如 G 没有 2 阶元,则每个非单位元 a 都有$a^{-1} \neq a$,去计算 $|G|$.

*10. 在 $U(\mathbf{Z}_n)$ 中,用 Lagrange 定理的推论(关于元素的阶).

11.6 的正因子有 1,2,3,6.因此 6 阶循环群$\langle a\rangle$的所有子群为:$\{e\}, \langle a^3\rangle, \langle a^2\rangle, \langle a\rangle$.

12. S_3 的所有子群为

$\{(1)\}, \langle (12)\rangle, \langle (13)\rangle, \langle (23)\rangle, \langle (123)\rangle, S_3$.

13.(1) A_4 的所有子群为

$\{(1)\}, \langle (12)(34)\rangle, \langle (13)(24)\rangle, \langle (14)(23)\rangle$,

$\langle (123)\rangle, \langle (124)\rangle, \langle (134)\rangle, \langle (234)\rangle$,

$\{(1),(12)(34),(13)(24),(14)(23)\}$、$A_4$.

*(2) 假如 H 是A_4的 6 阶子群,则 H 必含有 3 - 轮换,且 H 中 3 - 轮换的数目 r 为偶数,且 $r = 4$ 或 2.分别讨论 $r = 4, r = 2$ 的情

形，去得出矛盾.

*14. 证 $H \cap K = M$，则 $M < H$. 设 $H = \bigcup_{i=0}^{r-1} h_i M$，去证 $HK = \bigcup_{i=0}^{r-1} h_i K$，且 $h_i K \cap h_j K = \varnothing$ 当 $i \neq j$. 再计算 $|HK|$.

习题 1.3

1. 令 $f: \mathbf{R} \longrightarrow \mathbf{R}^+$

$$x \longmapsto e^x.$$

去证 f 是双射，且 f 保持运算.

2. 去计算 $\bar{2}^i$，$i = 2,3,4,5,6$. 从而知道 $\bar{2}$ 的阶为 6，由此出发去说明 $U(\mathbf{Z}_9) \cong \mathbf{Z}_6$.

3. 考察 $U(\mathbf{Z}_8)$ 是否为循环群，然后运用关于 4 阶群的类型的结论.

4. 考察棋盘的对称(性)群 G 是否为循环群.

*5. 让等边三角形的对称(性)群 D_3 作用在顶点集 $\Omega = \{1,2,3\}$ 上，可得 $\sigma \mapsto (123)$，$\tau \mapsto (12)$. 于是可建立 D_3 到 S_3 的一个映射 f. 易看出 f 是双射. 分别写出 D_3，S_3 的运算表(注意让 D_3 与 S_3 的元素的排列次序相对应)，比较这两张表可知 f 保持运算. 从而 $D_3 \cong S_3$.

6. 建立 G 到自身的一个映射 $\sigma: x \mapsto x^{-1}$.

充分性. 去证 σ 是双射，且保持运算.

必要性. 任取 $x, y \in G$，去证 $xy = yx$.

7. 利用交换群与非交换群不同构，同构映射保持元素的阶不变去讨论.

8. 由于 $V \cong \mathbf{Z}_2 \times \mathbf{Z}_2$，因此 $\mathbf{Z}_3 \times V \cong \mathbf{Z}_3 \times (\mathbf{Z}_2 \times \mathbf{Z}_2)$. 说明映射 $(a,(b,c)) \mapsto ((a,b),c)$ 是 $\mathbf{Z}_3 \times (\mathbf{Z}_2 \times \mathbf{Z}_2)$ 到 $(\mathbf{Z}_3 \times \mathbf{Z}_2) \times \mathbf{Z}_2$ 的一个同构映射，从而 $\mathbf{Z}_3 \times (\mathbf{Z}_2 \times \mathbf{Z}_2) \cong (\mathbf{Z}_3 \times \mathbf{Z}_2) \times \mathbf{Z}_2$. 又由于 $\mathbf{Z}_3 \times \mathbf{Z}_2 \cong \mathbf{Z}_6$，从而可说明 $(\mathbf{Z}_3 \times \mathbf{Z}_2) \times \mathbf{Z}_2 \cong \mathbf{Z}_6 \times \mathbf{Z}_2$. 最后说明 $\mathbf{Z}_6 \times \mathbf{Z}_2 \cong \mathbf{Z}_2 \times$

$\mathbf{Z}_6$. 利用同构关系的传递性即得所要证的结论.

9. 注意循环群与非循环群不同构. 利用第 8 题证明过程中阐述的结论可得

$$\mathbf{Z}_6 \times \mathbf{Z}_4 \cong (\mathbf{Z}_2 \times \mathbf{Z}_3) \times \mathbf{Z}_4 \cong \mathbf{Z}_2 \times (\mathbf{Z}_3 \times \mathbf{Z}_4) \cong \mathbf{Z}_2 \times (\mathbf{Z}_4 \times \mathbf{Z}_3)$$
$$\cong \mathbf{Z}_2 \times \mathbf{Z}_{12}.$$

* 10. D_{12} 有 12 阶元 σ,去计算 $D_4 \times \mathbf{Z}_3$, $A_4 \times \mathbf{Z}_2$ 有没有 12 阶元. 如果有的群有 12 阶元,再进一步比较 2 阶元的个数.

* 11. 当 n 是奇数时,求出 $D_n \times \mathbf{Z}_2$ 的一个 $2n$ 阶元$(\gamma, \overline{1})$,再指出 $D_n \times \mathbf{Z}_2$ 的一个 2 阶元$(\delta, \overline{1})$,去计算$(\delta, 1)(\gamma, \overline{1})(\delta, \overline{1})$. 由此推出, $D_n \times \mathbf{Z}_2$ 的元素可写成下述形式:

$$(\gamma, \overline{1})^i (\delta, 1)^j, \quad 0 \leqslant i < 2n, \quad j = 0, 1.$$

从而容易建立 D_{2n} 到 $D_n \times \mathbf{Z}_2$ 的一个映射 f. 去证 f 是同构映射.

* 12. (1) 由于 n 为奇数,因此 $-I \notin SO_n$,于是 $SO_n \cap \{I, -I\} = \{I\}$. 去证 $O_n = SO_n \cdot \{I, -I\}$.

(2) 利用第(1)小题结论,且注意 $\{I, -I\} \cong \mathbf{Z}_2$.

习题 1.4

1. (1) 只要证 f 保持运算;

(2) $\mathrm{Ker} f = \mathbf{Z}$; $\mathrm{Im} f$ 是复平面上的单位圆,记作 C.

2. (1) 去证 ψ 保持运算;

(2) $\mathrm{Ker}\psi = \mathbf{R}^+$, $\mathrm{Im}\psi$ 是复平面上的单位圆 C.

3. (1) 去证 σ 保持运算;

(2) $\mathrm{Ker}\sigma = SL_n(F)$; 说明 σ 是满射,从而 $\mathrm{Im}\sigma = F^*$.

(3) 由于 $SL_n(F) = \mathrm{Ker}\sigma$,因此 $SL_n(F) \lhd GL_n(F)$.

(4) 利用群同态基本定理.

4. (1) 设 $f_1(x) = k_1 x + b_1$, $f_2(x) = k_2 x + b_2$, $k_1 k_2 \neq 0$. 去证映射的乘积 $f_1 f_2$ 仍是一次函数,再用群的定义去验证.

(2) 设 $f_1(x) = x + b_1$, $f_2(x) = x + b_2$. 去证 $f_1f_2^{-1} \in H$. 从而 $H < G$. 任意给定 $f \in G$, 任取 $h \in H$, 去证 $fhf^{-1} \in H$. 从而 $H \triangleleft G$.

(3) 令 $\sigma: G \longrightarrow \mathbf{R}^*$

$$f \longmapsto k,$$

其中 $f(x) = kx + b$. 去证 σ 是满同态; 去求 $\mathrm{Ker}\sigma$; 再利用群同态基本定理.

5. 利用第 1 题的结论, 以及群同态基本定理.

6. 利用第 2 题的结论, 以及群同态基本定理.

7. 令 $\sigma: G \times G' \longrightarrow \mathbf{G}'$

$$(g, g') \longmapsto g'.$$

去证 σ 满同态; 去求 $\mathrm{Ker}\sigma$; 再利用群同态基本定理.

8. 由于 G 中每个元素 g 可唯一地表示成 $g = hk$, 其中 $h \in H$, $k \in K$. 于是令

$$\sigma: G \longrightarrow K$$

$$hk \longmapsto k.$$

去证 σ 是满同态; 去求 $\mathrm{Ker}\sigma$; 再利用群同态基本定理.

9. D_3 中, $|\langle\sigma\rangle| = 3$, 说明 $\langle\sigma\rangle \triangleleft D_3$. 于是有商群 $D_3/\langle\sigma\rangle$, 其阶为 2, 从而 $\langle\sigma\rangle \supseteq D'_3$, 进一步说明 $D'_3 = \langle\sigma\rangle$.

D_4 中, 去计算 $\sigma^i\sigma^2(\sigma_i)^{-1}$, $\tau\sigma^2\tau^{-1}$ 从而说明 $\langle\sigma^2\rangle \triangleleft D_4$. 于是有商群 $D_4/\langle\sigma^2\rangle$, 其阶为 4, 从而 $\langle\sigma^2\rangle \supseteq D'_4$. 说明 σ^2 是换位子, 从而 $\langle\sigma^2\rangle \subseteq D'_4$, 因此 $D'_4 = \langle\sigma^2\rangle$.

* 10. 类似于求 D_4 的换位子群的方法, 可求出

$D'_{2m+1} = \langle\sigma^2\rangle = \langle\sigma\rangle$, $D'_{2m} = \langle\sigma^2\rangle$.

11. 说明 $A_4 \triangleleft S_4$, 于是有商群 S_4/A_4, 其阶为 2. 因此 $A_4 \supseteq S'_4$, 说明每一个 3 - 转换 (ijk) 都是换位子, 从而 $A_4 \subseteq S'_4$. 因此 $S'_4 = A_4$.

* 12. 当 $n \geqslant 3$ 时, 与求 S'_4 的方法完全一样, 可得 $S'_n = A_n$.

*13. 当 $n\geqslant 5$ 时,对于 A_n 中任意一个 3 - 转换 $(a_1a_2a_3)$,取 $\sigma=(a_1a_3a_4a_2a_5)\in A_n$, $\tau=(a_1a_5a_2)\in A_n$. 说明 $(a_1a_2a_3)$ 是换位子. 从而 $A_n\subseteq A_n'$, 于是 $A_n'=A_n$.

14. $S_4\rhd A_4\rhd V\rhd\{e\}$.

*15. 考虑 G 到 U_2 的一个映射 ψ,它把偶置换映成 1,把奇置换映成 -1,去证 ψ 是满同态;去求 $\mathrm{Ker}\psi$;然后用群同态基本定理.

*16. (1) 说明 $\sigma^{-1}(H')$ 非空. 任取 $g_1,g_2\in\sigma^{-1}(H')$,去证 $g_1g_2^{-1}\in\sigma^{-1}(H')$,于是 $\sigma^{-1}(H')<G$. 易证 $K\subseteq\sigma^{-1}(H')$.

(2) 考虑映射 $\psi: H'\longmapsto\sigma^{-1}(H')$. 去证 ψ 是满射,再证 ψ 是单射.

*17. 任意给定 $a,b\in\{1,2,\cdots,n\}$. 任取一个 3 - 转换 (ijk),去证 (ijk) 可表示成 $(abl)^j$, $(1\leqslant l\leqslant n, l\neq a,b, 1\leqslant j\leqslant 2)$ 的乘积. 从而 A_n 可由集合 $M=\{(abl)\mid 1\leqslant l\leqslant n, l\neq a,b\}$ 生成. 即 $A=\langle M\rangle$.

任取 A_n 的一个正规子群 $N\neq\{e\}$,要证 $N=A_n$.

情形 1 设 N 含有一个 3 - 轮换 (abc),去证 $(abk)\in N$,其中 $k\neq a,b,c$,从而 $M\subseteq N$. 因此 $\langle M\rangle\subseteq N$.

情形 2 设 N 中含有 σ,其轮换分解式中至少有一个 r - 轮换,其中 $r\geqslant 4$. 即 $\sigma=(a_1a_2\cdots a_r)\sigma_1$. 令 $\tau=(a_1a_2a_3)$. 去证 $(a_1a_2a_r)\in N$. 归结为情形 1.

情形 3 设 N 中含有 σ,其轮换分解式中至少有两个 3 - 轮换. 即 $\sigma=(a_1a_2a_3)(a_4a_5a_6)\sigma_1$. 令 $\tau=(a_1a_2a_4)$. 去证 $(a_1a_4a_2a_6a_3)\in N$. 归结为情形 2.

情形 4 设 N 含有 σ,其轮换分解式为 $\sigma=(a_1a_2a_3)\sigma_1$,其中 σ_1 是一些不相交的对换的乘积. 去证 $(a_1a_3a_2)\in N$. 归结为情形 1.

情形 5 设 N 含有 σ,它是偶数个不相交的对换的乘积,即 $\sigma=(a_1a_2)(a_3a_4)\sigma_1$,其中 σ_1 是偶数个不相交的对换的乘积. 取 $\tau=$

$(a_1a_2a_3)$. 去证$(a_1a_3)(a_2a_4) \in N$. 进一步去证$(a_1a_3b) \in N$，对某个 b 不在 a_1, a_2, a_3, a_4. 归结为情形 1.

综上述得，$N = A_n$，因此 A_n 是单群.

* 18. 由第一同构定理可得结论.

* 19. 计算$|A_n\langle(12)\rangle|$，可得 $S_n = A_n\langle(12)\rangle$.

习题 1.5

1. 去证$(n + m) \circ x = n \circ (m \circ x)$, $0 \circ x = x$.

2. 去证$(n + m) \circ x = n \circ (m \circ x)$, $0 \circ x = x$.

3. 去证 σ 是双射，且保持运算.

4. 利用与所有 n 级可逆矩阵可交换的矩阵一定是数量矩阵(参看《高等代数(上册)》，丘维声编著，高教社 1996 年出版，第 238 页，补充题四的第 4 题)，可得

$$Z(GL_n(F)) = \{kI \mid k \in F^*\}.$$

* 5.(1) 任取 G 中两个元素 σ_1, σ_2，其中

$$\sigma_i(z) = \frac{a_iz + b_i}{c_iz + d_i} = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix}, i = 1, 2.$$

去证 $\sigma_1\sigma_2 \in G$. 然后按照群的定义去验证 G 是一个群.

(2) 令 $\psi: GL_2(\mathbf{C}) \longrightarrow G$

$$A \longmapsto \sigma_A,$$

其中 $\sigma_A(z) = A\begin{pmatrix} z \\ 1 \end{pmatrix}$. 去证 ψ 是满同态；去求 $\mathrm{Ker}\psi$；然后利用群同态基本定理.

6. 设 $G/Z(G) = \langle aN \rangle$，其中 $N = Z(G)$. 任取 $x, y \in G$. 去证 $xyx^{-1}y^{-1} = e$.

7. 去推导 $\sigma' \in Z(D_{2m-1}) \Longleftrightarrow \tau\sigma'\tau^{-1} = \sigma' \Longleftrightarrow \cdots$ 可求出 $Z(D_{2m-1}) = \{I\}$；类似地，可求出 $Z(D_{2m}) = \{I, \sigma^m\}$.

*8. 设 $\tau \in Z(S_n)$. 则 $\tau(1i)\tau^{-1} = (1i)$, $i = 2,3,\cdots,n$. 由此推出, $\tau = (1)$. 因此 $Z(S_n) = \{(1)\}$, 其中 $n \geqslant 3$.

9. $U_6 = \langle \xi \rangle$, 其中 $\xi = e^{i\frac{\pi}{3}}$. U_6 的生成元恰有两个: ξ, ξ^5, 由于自同构把生成元映成生成元. 因此, $\mathrm{Aut}(U_6)$ 只有两个元素.

$$U_9 = \langle \zeta \rangle, \text{其中 } \zeta = e^{i\frac{2\pi}{9}},$$

U_9 的生成元恰有 6 个. 由此可求出 $\mathrm{Aut}(U_9)$ 是 6 阶循环群.

10. $\mathbf{Z}_2 \times \mathbf{Z}_2$ 有三个 2 阶元: $(\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})$. 自同构 τ 把 2 阶元映成 2 阶元. 因此 τ 有 6 种可能的选择. 它们分别对应于 S_3 的 6 个置换, 去验证 τ 的每一种选择都是 $\mathbf{Z}_2 \times \mathbf{Z}_2$ 的一个自同构. 因此 $\mathrm{Aut}(\mathbf{Z}_2 \times \mathbf{Z}_2)$ 有 6 个元素. 进一步可证 $\mathrm{Aut}(\mathbf{Z}_2 \times \mathbf{Z}_2) \cong S_3$.

*11. S_3 有 3 个 2 阶元. 自同构 τ 把 2 阶元映成 2 阶元. 因此 τ 有 6 种可能的选择, 它们分别对应于 S_3 的 6 个置换. 去验证 τ 的每一种选择都是 S_3 的一个自同构. 进一步可证 $\mathrm{Aut}(S_3) \cong S_3$.

*12. 设 $\sigma \in \mathrm{Aut}(G)$. 任取 $a \in Z(G)$, 对于任意 $x \in G$, 去证 $\sigma(a)x\sigma(a)^{-1}x^{-1} = e$. 从而 $\sigma(a) \in Z(G)$. 因此 $\sigma(Z(G)) = Z(G)$.

任取 $x, y \in G$, 去证 $\sigma(xyx^{-1}y^{-1}) \in G'$. 从而 $\sigma(G') \subseteq G'$. 因此 $\sigma(G') = G'$.

13. 从第 7 题知, $Z(D_5) = \{I\}$. 于是 $C_{D_5}(\sigma^i) = \langle \sigma \rangle, 1 \leqslant i \leqslant 4$; $C_{D_5}(\tau) = \{I, \tau\}$; $C_{D_5}(\sigma^j\tau) = \{I, \sigma^j\tau\}, 1 \leqslant j \leqslant 4$. 从而可求出 $|D_5(\sigma^i)|, 1 \leqslant i \leqslant 4$; $|D_5(\sigma^j\tau)|, 0 \leqslant j \leqslant 4$. 进一步可求出, $D_5(\sigma) = \{\sigma, \sigma^4\}, D_5(\sigma^2) = \{\sigma^2, \sigma^3\}$. 又 $D_5(I) = \{I\}$. 从而 $D_5(\tau) = \{\sigma^j\tau \mid 0 \leqslant j \leqslant 4\}$. 于是 D_5 共有 4 个共轭类.

从第 7 题知道, $Z(D_6) = \{I, \sigma^3\}$. 类似于上述方法可求出, $D_6(\sigma) = \{\sigma, \sigma^5\}, D_6(\sigma^2) = \{\sigma^2, \sigma^4\}, D_6(\sigma^3) = \{\sigma^3\}, D_6(I) =$

$\{I\}$, $D_6(\tau)=\{\tau,\sigma^2\tau,\sigma^4\tau\}$, $D_6(\sigma\tau)=\{\sigma\tau,\sigma^3\tau,\sigma^5\tau\}$. 于是 D_6 共有 6 个共轭类.

* 14. 类似于求 D_5 的共轭类的方法可得 D_{2m-1} 有 $m+1$ 个共轭类,它们是:

$$\{I\},\{\sigma^i,\sigma^{2m-1-i}\},\quad i=1,2,\cdots,m-1,$$
$$\{\sigma^j\tau\mid 0\leqslant j\leqslant 2m-2\}.$$

类似于求 D_6 的共轭类的方法可得 D_{2m} 有 $m+3$ 个共轭类,它们是

$$\{I\},\{\sigma^m\},\{\sigma^i,\sigma^{2m-i}\},\quad i=1,2,\cdots,m-1,$$
$$\{\tau,\sigma^2\tau,\sigma^4\tau,\cdots,\sigma^{2(m-1)}\tau\},\{\sigma\tau,\sigma^3\tau,\cdots,\sigma^{2m-1}\tau\}.$$

15. (1) 必要性. 利用习题 1.1 的第 12 题的结论.

充分性. 仍利用习题 1.1 的第 12 题的结论.

(2) 从第(1)小题的结论和置换的型的定义立得.

16. 4 的分拆有 5 个. 从而 S_4 有 5 个共轭类,它们的代表分别是:(1234),(123),(12)(34),(12),(1). 相应的共轭类的元素个数为 6,8,3,6,1.

17. A_4 中 σ_1 与 σ_2 共轭的必要条件是 σ_1 与 σ_2 同型,但这不是充分条件. 例如,(123)与(132)虽然同型,但它们在 A_4 中不共轭. 用共轭的必要条件并且经过检查得,A_4 有 4 个共轭类,它们的代表分别是:

$$(1),(12)(34),(123),(132);$$

相应的共轭类的元素个数为 1,3,4,4.

18. n - 轮换 σ 的共轭类的元素个数为 $(n-1)!$. 从而 $|C_{S_n}(\sigma)|=n$. 由此推出 $C_{S_n}(\sigma)=\langle\sigma\rangle$.

19. O_2 的元素只有两种形式:

$$A_\theta=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix},\quad B_\varphi=\begin{pmatrix}\cos\varphi & \sin\varphi\\ \sin\varphi & -\cos\varphi\end{pmatrix},$$

其中 $0\leqslant\theta<2\pi$, $0\leqslant\varphi<\pi$(参看《高等代数(下册)》),丘维声编著,

高教社 1996 年出版，第 369 页）. O_2 里两个元素共轭也就是这两个矩阵正交相似. 从而可求出 O_2 的全部共轭类为

$$\{I\},\{A_\pi\},\{B_\varphi \mid 0 \leqslant \varphi < 2\pi\},\{A_\theta, A_{2\pi-\theta}\}, 0 < \theta < \pi.$$

20. 必要性. 设 $H \triangleleft G$. 则对于 $h \in H$，所有的 $g \in G$，有 $ghg^{-1} \in H$. 即 H 包含 h 的共轭类.

充分性. 任取 $h \in H$，对于所有的 $g \in G$，有 $ghg^{-1} \in H$. 从而 $gHg^{-1} \subseteq H$. 因此 $H \triangleleft G$.

*21. (1) 5 的分拆有 7 个，因此 S_5 有 7 个共轭类. 它们的代表分别是

$$(1),(12),(12)(34),(123),(123)(45),(1234),(12345).$$

相应的共轭类的元素数目为 1,10,15,20,20,30,24.

(2) S_5 的正规子群应当是一些共轭类的并集，又子群的阶是 $|S_5|$ 的因子，且子群包含 S_5 的单位元. 由此推出 S_5 的非平凡正规子群只有 A_5.

22. 因为 $N \triangleleft G$，所以有群 G 在 N 上的共轭作用. 用 Ω_0 表示 G 的不动点集，去求 Ω_0.

23. 由轨道 — 稳定子定理立即得到.

24. 利用 H 的共轭子群的个数等于 $[G:N_G(H)]$. 去考察 $|\bigcup_{g \in G} gHg^{-1}|$. 然后用反证法.

*25. 考虑群 G 在集合 G 上的左平移. 则 G 到 S_{2k} 有一个同态 ψ，且 $G \cong \mathrm{Im}\psi$. $|\mathrm{Im}\psi| = |G| = 2k$. 因此 $\mathrm{Im}\psi$ 必有 2 阶元，设为 $\psi(a)$. 求 $\psi(a)$ 的轮换分解式. 说明 $\psi(a)$ 是奇置换. 然后用习题 1.4 的第 14 题结论.

*26. 考虑群 G 在左商集 $(G/H)_l$ 上的左平移. 从而 G 到 S_n 有一个同态 ψ. 分情形讨论 $\mathrm{Ker}\psi$.

*27. 设 G 有一个指数为 p 的子群 H. 考虑群 G 在左商集 $(G/H)_l$ 上的左平移. 从而 G 到 S_p 有一个同态 ψ，去证 $\mathrm{Ker}\psi = H$.

*28. 正方体的旋转对称(性)群 G 作用在 6 个面组成的集合 W 上,从而 G 的每个元素诱导了 W 的一个置换,然后用 Pólya 定理得,轨道条数为

$$r = \frac{1}{24}(6\times 2^3 + 3\times 2^4 + 8\times 2^2 + 6\times 2^3 + 2^6) = 10.$$

因此真正不同的染色方案有 10 个.

*29. 在轨道 - 稳定子定理中已证明 $\psi:(a\circ x)\mapsto aG_x$ 是 $G(x)$ 到 $(G/G_x)_l$ 的一个双射. 由于 G 在 Ω 上的作用是传递的,因此 ψ 是 Ω 到 $(G/G_x)_l$ 的一个双射,按照等价作用的定义去验证 G 在 Ω 上的传递作用与 G 在 $(G/G_x)_l$ 上的左平移等价.

*30. 验证结合律成立. 说明 (n,h) 有逆元. 从而 $N\times H$ 是一个群,验证 $\widetilde{N}\lhd N\rtimes H$. 显然 $n\mapsto(n,e)$ 是 N 到 $\widetilde{N}$ 的一个同构映射,从而 $N\cong\widetilde{N}$.

*31. 去证 $[(g_1,h_1)(g_2,h_2)]\circ(x,y) = (g_1,h_1)\circ[(g_2,h_2)\circ(x,y)]$;$(e,e)\circ(x,y)=(x,y)$. 从而这给出了 $G\times H$ 在 $\Omega\times W$ 上的一个作用. 可证

$$(G\times H)(x,y) = G(x)\times H(y);$$
$$(G\times H)_{(x,y)} = G_x\times H_y.$$

习题 1.6

1. 去计算 G 的 Sylow 37 - 子群的个数.

2. 与本节例 1 的证法类似.

3. 去计算 G 的 Sylow 7 - 子群的个数 r. 分情形讨论. $r=1$ 时,G 的 Sylow 7 - 子群是正规子群. $r=8$ 时,去计算 G 的 7 阶元的个数.

4. 去计算 G 的 Sylow 5 - 子群的个数 r. 分情形讨论. $r=1$ 时,G 的 Sylow 5 - 子群是正规子群. $r=6$ 时,去计算 G 的 5 阶元的个

数；并且去求 G 的 Sylow 3－子群的个数 t. 进一步分情形讨论：$t=1$ 时，G 的 Sylow 3－子群是正规子群；$t=10$ 时，去计算 G 的 3 阶元的个数. 找出矛盾.

5. 从本节例 2 即得.

6. 从本节例 2 即得.

7. 去计算 G 的 Sylow 5－子群和 Sylow 3－子群的个数，可知 G 的 Sylow 5－子群和 Sylow 3－子群都是正规子群，分别记作 K, H. 说明 $H=\langle a\rangle, K=\langle b\rangle, H\cap K=\{e\}$. 去证 $ab=ba$. 进而求 $|ab|$，便可知 15 阶群的类型.

8. 类似于第 7 题的方法.

*9. 计算 21 阶群 G 的 Sylow 7－子群的个数 r；计算 G 的 Sylow 3－子群的个数 t. 分情形讨论：$t=1$ 时，类似于第 7 题的方法可知，G 是循环群. $t=7$ 时，G 是非交换群. 取 G 的一个 Sylow 3－子群 H. 设 $H=\langle b\rangle$. 设 G 的 Sylow 7－子群 $N=\langle a\rangle$. 说明 $N\cap H=\{e\}$. 计算 $|NH|$. 从而得 $NH=G$. 任取 $\sigma\in \mathrm{Aut}(N)$，则 σ 把 N 的生成元映成生成元，从而 $\sigma(a)$ 有 6 种可能的选择. 易验证 σ 的每一种选择都是 $\langle a\rangle$ 的自同构. 可求出 $Aut(N)$ 有一个 6 阶元，记作 σ. 由于 $N\lhd G$，因此群 H 在 N 上有共轭作用，它引起了 H 到 S_N 的一个同态 ψ. 说明 $\psi(h)$ 是 N 的一个自同构. 从而 $\mathrm{Im}\psi\subseteq \mathrm{Aut}(N)$. 即 ψ 可看成是 H 到 $\mathrm{Aut}(N)$ 的一个同态. 计算 $|\psi(b)|$. 从而得出 $\psi(b)=\sigma^2$ 或 σ^4. 不妨设 $\psi(b)=\sigma^2$. 从而 $bab^{-1}=a^2$. 因此 $G=\langle a,b\mid a^7=b^3=e, bab^{-1}=a^2\rangle$. 令

$$f:\ N\rtimes H\to G$$
$$(n,h)\mapsto nh,$$

去证 f 是一个同构映射. 从而 $N\rtimes H\cong G$. 由于 $N\cong \mathbf{Z}_7, H\cong \mathbf{Z}_3$，且 $\mathbf{Z}_7$ 与 $\mathbf{Z}_3$ 可作半直积，从而 $G\cong \mathbf{Z}_7\rtimes \mathbf{Z}_3$.

综上述得，21 阶群或者同构于 $\mathbf{Z}_{21}$，或者同构于 $\mathbf{Z}_7\rtimes \mathbf{Z}_3$.

10. 设 pq 阶群 G 的 Sylow q - 子群的个数为 r，求 r，可知 Sylow q - 子群正规，记作 N. 计算 G 的 Sylow p - 子群的个数 t. 分情形讨论：(1) 如果 $q \not\equiv 1(\mathrm{mod}\ p)$，则 $t = 1$. 此时与第 7 题类似的方法可得出，G 是 pq 阶循环群.

(2) 如果 $q \equiv 1(\mathrm{mod}\ p)$，则 $t = 1$ 或 $t = q$，当 $t = 1$ 时，由第(1)小题知道，G 是循环群. 当 $t = q$ 时，G 不是交换群，且 G 有正规 Sylow q - 子群 N.

*11. 情形 1. $p > q$. 去计算 p^2q 阶群 G 的 Sylow p - 子群的个数，可知 Sylow p - 子群正规.

情形 2，$p < q$，对 G 的 Sylow q - 子群的个数 t 分情形讨论；

(i) $t = 1$，此时 G 的 Sylow q - 子群正规.

(ii) $t > 1$，且 $t = 1 + ql \mid p^2$. 可推出 $t = p^2$. 去计算 G 的 q 阶元的个数. 考虑剩下的元素.

12. 由于 $|G| = p^3$，因此 $|Z(G)|$ 等于 p 或 p^2 或 p^3，排除 p^2，p^3 这两种可能情形. 因此 $|Z(G)| = p$. 考虑商群 $G/Z(G)$. 由此出发求 G'. 可得 $G' = Z(G)$.

*13. $|S_p| = p!$，说明 S_p 的 Sylow p - 子群的阶为 p，于是必形如 $\langle\sigma\rangle$，其中 σ 是 p 阶元，从而 σ 为 p - 轮换. 从 S_p 中 p - 轮换的个数，去求 S_p 的 Sylow p - 子群的个数 r. 据 Sylow 第三定理可得出所要的结论.

*14. 任取 $g \in G$. 因为 $P \subseteq N$. 所以 $gPg^{-1} \subseteq N$. 从而 gPg^{-1} 也是 N 的一个 Sylow p - 子群. 从而存在 $n \in N$，使得 $n(gPg^{-1})n^{-1} = P$. 由此推出 $ng \in N_G(P)$. 进而可得所要的结论.

*15. 设 $|G| = 2^l m$，$(m, 2) = 1$，$l > 0$，设 G 有一个循环的 Sylow 2 - 子群 $H = \langle a\rangle$. 考虑群 G 在集合 G 上的左平移，由此得到 G 到 $S_{2^l m}$ 的一个同态 φ. 说明 $G \cong \mathrm{Im}\varphi$. 去证 $\mathrm{Im}\varphi$ 含有奇置换，则据习题 1.4 的第 14 题得，$\mathrm{Im}\varphi$ 必有指数为 2 的子群 K'，从而 $\varphi^{-1}(K')$ 是 G 的指数为 2 的子群. 为了证 $\mathrm{Im}\varphi$ 含有奇置换，考虑 $\varphi(a)$.

习题 1.7

1. $12 = 2^2 \times 3$,从而 12 阶 abel 群的初等因子只有 2 种可能:$\{2^2, 3\}$,$\{2,2,3\}$.因此 12 阶 abel 群有两种互不同构的类型.它们的代表是:$\mathbf{Z}_{2^2} \times \mathbf{Z}_3, \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$.

2. 108 阶 abel 群有 6 种互不同构的类型,代表是:

$\mathbf{Z}_{2^2} \times \mathbf{Z}_{3^3}$,　$\mathbf{Z}_{2^2} \times \mathbf{Z}_3 \times \mathbf{Z}_{3^2}$,　$\mathbf{Z}_{2^2} \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$,

$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{3^3}$,　$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_{3^2}$,　$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$.

3. 360 阶 abel 群有 6 种互不同构类型,读者可自己写出它们的代表.

4. 144 阶 abel 群有 10 种互不同构的类型,读者可自己写出它们的代表.

5. 216 阶 abel 群有 9 种互不同构的类型,读者可自己写出它们的代表.

6. (1) $\{2,2^2,3,5,5,5\}$;

(2) $\{2,2^2,3,7,7\}$;

(3) $\{2,2,2^4,3,3^2,7\}$.

7. 100 阶 abel 群有 4 种互不同构类型,请读者自己写出它们的代表.

(1) 从上述代表看出,每一种类型都有 10 阶元;

*(2) 100 阶 abel 群 G 不含阶大于 10 的元素当且仅当 G 的初等因子为$\{2,2,5,5\}$.

*8. 由已知条件,$|G| = n = p_1 p_2 \cdots p_s$,其中 $p_1, \cdots, p_s$ 是两两不同的素数.考虑 G 的初等因子有几种可能.

*9. 设 abel p - 群 G 的阶为 p^m.设

$$G \cong \mathbf{Z}_{p^{k_1}} \times \mathbf{Z}_{p^{k_2}} \times \cdots \times \mathbf{Z}_{p^{k_s}},$$

其中 $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_s$.假如 $s > 1$,去计算 G 的 p 阶元的个数至少

有多少.

*10. V 的加法群 $G = \{(a_1, a_2, \cdots, a_n) \mid a_i \in \mathbf{Z}_2, 1 \leqslant i \leqslant n\}$

$$= \underbrace{\mathbf{Z}_2 \times \mathbf{Z}_2 \times \cdots \times \mathbf{Z}_2}_{n\text{个}}.$$

于是 G 的初等因子为 $\{2, 2, \cdots, 2\}$. 从而 G 是初等 abel 2 − 群.

*11. 与第 10 题类似, V 的加法群是初等 abel p − 群.

习题 1.8

1. (1) $w_1 = x^{-1}y^2z^{-2}$;　　(2) $w_2 = z^2y^{-2}x^3z^{-2}$;

(3) $w_3 = z^2yz^4y^{-1}$.

2. $\overline{w_1}\,\overline{w_2} = x^2z^{-2}$; $\overline{w_1}\,\overline{w_2}\,\overline{w_3} = x^2yz^4y^{-1}$.

*3. (1) 取 $a = (12)$, $b = (1234)$. 据习题 1.2 的第 5 题知道, $S_4 = \langle (12), (1234) \rangle$. 因此 $X = \{a, b\}$ 是 S_4 的一个生成元集. 令 $R = \{a^2, b^4, (ab)^3\}$. 用 M 表示 $F(X)$ 中由 R 生成的正规子群. 用 N 表示从 $F(X)$ 到 S_4 的同态 φ 的核. 我们要证 $M = N$. 先说明 $M \subseteq N$. 然后据 §4 的第二同构定理得

$$(F(X)/M)/(N/M) \cong F(X)/N.$$

又由于 $F(X)/N \cong S_4$. 因此 $|F(X)/M| \geqslant |S_4| = 24$.

显然 $F(X)/M = \langle aM, bM \rangle$. 并且它们满足

$$(aM)^2 = M, \quad (bM)^4 = M, \quad (abM)^3 = M.$$

去证 $|F(X)/M| < 48$. 从而 $|N/M| < 2$, 因此 $N = M$, 从而 $F(X)/M \cong S_4$. 于是 $S_4 = \{a, b \mid a^2, b^4, (ab)^3\}$.

(2) 取 $a = (12)$, $c = (234)$. 由于 $b = (1234) = ac$, 因此 $X_1 = \{a, c\}$ 也是 S_4 的一个生成元集. 令 $R_1 = \{a^2, c^3, (ac)^4\}$. 用 M_1 表示 $F(X_1)$ 中由 R_1 生成的正规子群. 由于 $c = ab$, 因此 $F(X_1) = F(X)$, 去证 $M_1 = M$. ($F(X)$, M 见第(1)小题.) 从而 $F(X_1)/M_1 = F(X)/M \cong S_4$. 于是

$$S_4 = \{a, c \mid a^2, c^3, (ac)^4\}.$$

*4. 与第 3 题的第(1)小题的方法类似.

5.

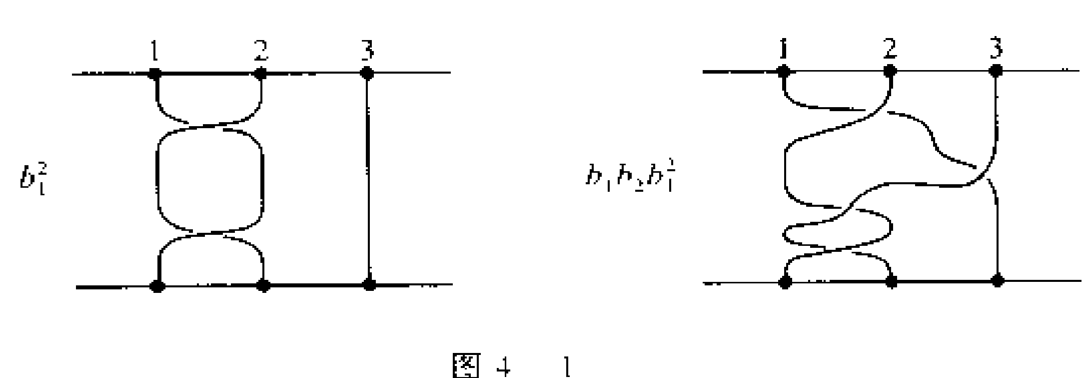


图 4－1

6. b_1^2 产生置换(1)；$b_1b_2b_1^2$ 产生置换(132).

7. 第 6 题中的辫子 $b_1b_2b_1^2$ 与 §8 的图 1－9 的辫子 b 都产生置换(132).

8.

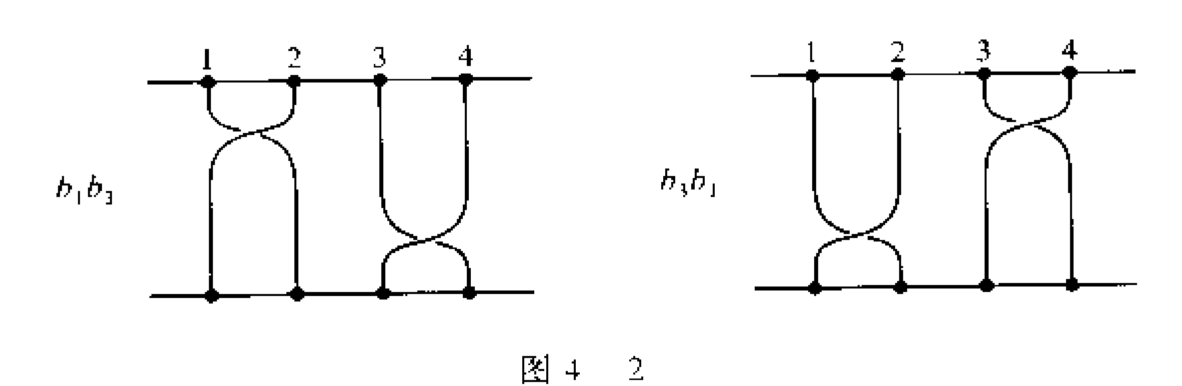


图 4－2

从图 4－2 看出，$b_1b_3 = b_3b_1$.

*9. 把 **Z** 里的加法运算写成乘法的形式，即把整数 $m = m1$ 写成 1^m，并且在 **Z** * **Z** 中，把前一个 **Z** 里的 m 写成 1^m，把后一个 **Z** 里的 m 写成 $\bar{1}^m$，以表明它们是不同的元素.

在 **Z** * **Z** 与 F_2 之间建立一个对应法则，去证这是同构映射.

第二章 环

习题 2.1

1. 去证 S 对减法、乘法封闭. S 的单位元是 E_{11}.

2. 设 $R=\{a_1,a_2,\cdots,a_n\}$. 任取 R 的一个非零元 a_i，去证存在某个 a_j 使得 $a_ia_j=1$，从而 a_i 可逆.

*3. 去证 $\mathbf{H}$ 对矩阵的减法、乘法封闭，因此 $\mathbf{H}$ 是环 $M_2(\mathbf{C})$ 的一个子环. 显然，单位矩阵 $I\in\mathbf{H}$. 对任意 $A\in\mathbf{H}$，且 $A\neq 0$，证明 A 是可逆矩阵，并且 $A^{-1}\in\mathbf{H}$. 从而 $\mathbf{H}$ 的每个非零元可逆. 因此 $\mathbf{H}$ 是一个除环.

4. 如果 $1\in I$，则 $\forall r\in R$，有 $r=r\cdot 1\in I$.

5. 用第 4 题的结论.

6. 任取 R 的一个非零元 a，由已知条件得，$(a)=R$. 去证 a 可逆.

7. 设 $r_1,r_2\in \operatorname{rad}I$，则存在 $n_1n_2\in\mathbf{Z}^+$，使得 $r_1^{n_1}\in I$，$r_2^{n_2}\in I$. 利用二项式定理去证 $(r_1-r_2)^{n_1+n_2}\in I$，从而 $r_1-r_2\in\operatorname{rad}I$. 易证 $\forall r\in R$，有 $(rr_1)^{n_1}\in I$，从而 $rr_1\in\operatorname{rad}I$.

8. 由于 a 是幂零元，因此存在正整数 n 使得 $a^n=0$. 易证 $1-a$ 可逆.

9. 用 J 表示所有幂零元组成的集合. 易看出，$J=\operatorname{rad}\{0\}$. 于是由第 7 题立得结论.

*10. 任取 $M_n(D)$ 的一个理想 J，设 $J\neq(0)$. 去证 $J=M_n(D)$. 为此只要证 $E_{ij}\in J$，$1\leqslant i,j\leqslant n$. 从而对于 $M_n(D)$ 中任一矩阵 $B=(b_{ij})$，有

$$B=\sum_{i=1}^{n}\sum_{j=1}^{n}b_{ij}E_{ij}\in J.$$

习题 2.2

1. 设 $\alpha = a + bi, \beta = c + di$，则

$$A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

$$= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$= aE + bI + cJ + dK,$$

其中

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

易证 A 表示成 $aE + bI + cJ + dK$ 的方式唯一. 令

$$\sigma : R \longrightarrow \mathbf{H}$$

$$A = aE + bI + cJ + dK \longmapsto a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}.$$

去证 σ 是双射，且保持加法，乘法运算.

2. (1)，(2) 直接按照理想的定义去验证.

3. 这队士兵的人数为 $116 + 105l (l \in \mathbf{N})$. 需依据这队士兵是相当于一个连(或一个团，一个师，一个军，…) 来具体确定人数.

4. $\mathbf{Z}/(35)$ 中，$\bar{1}$ 的平方根恰有 4 个：$\pm\bar{1}, \pm\bar{6}$；$\bar{4}$ 的平方根恰好有 4 个：$\pm\bar{2}, \pm\overline{12}$.

5. 在 $\mathbf{Z}/(35)$ 中，$\bar{2}, \bar{3}$ 都没有平方根. 提示：

$$(a + (35))^2 = 2 + (35)$$

$$\Longleftrightarrow = (a + (5))^2 = 2 + (5) \text{ 且 } (a + (7))^2 = 2 + (7).$$

*6. 利用本章 §1 的命题 2.

习题 2.3

1. 设 I 是 $F[x]$ 的一个理想，且 $I \neq (0)$. 在 I 的非零多项式中

取一个次数最低的多项式 $m(x)$，去证 $I=(m(x))$.

2. 据素理想的定义可证得结论.

*3. 环 $\mathbf{Z}$ 到 $\mathbf{Z}/(30)$ 有一个自然满同态 $\pi: k\mapsto k+(30)$，且 $\mathrm{Ker}\pi=(30)$. 利用本节的定理4（设 R 和 R' 都是有单位元的交换环，且 $1\neq 0, 1'\neq 0'$. 如果环 R 到 R' 有一个满同态 σ，则 $\mathrm{Spec}R'$ 到 R 的包含 $\mathrm{Ker}\sigma$ 的所有素理想组成的集合有一个一一对应 $\psi: P'\mapsto\sigma^{-1}(P')$；并且对于 R 的包含 $\mathrm{Ker}\sigma$ 的任一素理想 P，有 $\psi(\sigma(P))=P$）. 先求出 $\mathbf{Z}$ 的包含(30)的全部素理想为(2),(3),(5)；然后可得出

$$\mathrm{Spec}\mathbf{Z}/(30)=\{(2)/(30),(3)/(30),(5)/(30)\}.$$

4. 由于 $p(x)$ 不可约，因此 $(p(x))$ 是 $F[x]$ 的一个极大理想. 从而 $F[x]/(p(x))$ 是一个域.

5. 由于 $f(x)$ 可约，因此

$$f(x)=f_1(x)f_2(x), \deg f_i(x)<\deg f(x), i=1,2.$$

去证 $f_i(x)+(f(x))$ 是 $F[x]/(f(x))$ 的非平凡的零因子.

6. 首先找 $\mathbf{Z}_2[x]$ 中一个2次不可约多项式 $m(x)=x^2+x+1$，于是 $\mathbf{Z}_2[x]/(m(x))$ 是含有4个元素的域. 令 $u=x+(m(x))$，则

$$\mathbf{Z}_2[x]/(m(x))=\{0,1,u,1+u\}.$$

说明 u^2+u+1 是 $\mathbf{Z}_2[x]/(x^2+x+1)$ 的零元素，于是 $u^2+u+1=0$. 从而 $u^2=1+u$. 由此可求出加法表，乘法表.

7. 在 $\mathbf{Z}_3[x]$ 中找出一个2次不可约多项式 $m(x)$，则 $\mathbf{Z}_3[x]/(m(x))$ 是含9个元素的有限域.

8. 在 $\mathbf{Z}_2[x]$ 中找一个3次不可约多项式 $m(x)$，则 $\mathbf{Z}_2[x]/(m(x))$ 是含8个元素的有限域.

*9. 设 I 是 R 的一个理想，且 $I\supsetneqq(4)$，去证 $I=R$. 去证 $2+(4)$ 是 $R/(4)$ 的一个非平凡的零因子.

*10. (1) 令

$$\sigma: \mathbf{Z}\longrightarrow\mathbf{Z}e$$

$$n \mapsto ne.$$

易证 σ 是一个满同态. 从而

$$\mathbf{Z}/\mathrm{Ker}\sigma \cong \mathbf{Z}e.$$

然后利用本节命题 1.

(2) 如果 R 是整环, 则 $\mathbf{Z}e$ 也是整环, 然后利用本节定理 3.

* 11. 据习题 2.1 的第 9 题, R 的幂零根 $\mathrm{rad}(0)$ 是由 R 的所有幂零元组成的集合. 任取 R 的一个幂零元 a, 去证 a 属于 R 的任一素理想 P. 从而 $a \in \bigcap_{P \in \mathrm{Spec}R} P$.

反之, 设 a 为 R 的任一非幂零元. 设 S 为 R 中与集合 $\{a^n \mid n \in \mathbf{Z}^+\}$ 的交为空集的所有理想组成的集合. 由于 $(0) \in S$, 因此 S 非空集. S 对于集合的包含关系成为一个偏序集. 任取 S 的一条链

$$T = \{I_\alpha \mid \alpha \in J\}, \text{其中 } J \text{ 为指标集},$$

即 T 中每一对集合 I_α, I_β 都有 $I_\alpha \subseteq I_\beta$ 或者 $I_\beta \subseteq I_\alpha$. 令 $A = \bigcup_{\alpha \in J} I_\alpha$. 易证 A 是 R 的一个理想, 且 A 与 $\{a^n \mid n \in \mathbf{Z}^+\}$ 的交为空集. 因此 $A \in S$. 显然 A 是 T 的一个上界. 据 Zorn 引理, S 有一个极大元素 P. 用反证法可以证 P 是素理想: 若 P 不是素理想, 则存在 $b, c \in R$ 使得 $bc \in P$ 但是 $b \overline{\in} P$ 且 $c \overline{\in} P$. 令 $H = (b) + P, K = (c) + P$. 可证 $P \subseteq H, P \neq H$. 因此 $H \overline{\in} S$. 从而存在 $a^t \in S$. 同理可证 $K \overline{\in} S$, 从而存在 $a^s \in K$, 于是 $a^{t+s} \in HK$. 但是

$$HK = (b)(c) + (b)P + P(c) + PP \subseteq P.$$

因此 HK 与 $\{a^n \mid n \in \mathbf{Z}^+\}$ 的交为空集, 矛盾. 所以 P 是 R 的一个素理想, 且 P 与 $\{a^n \mid n \in \mathbf{Z}^+\}$ 的交为空集, 从而 $a \overline{\in} P$. 因此 $a \overline{\in} \bigcap_{I \in \mathrm{Spec}R} I$.

综上述得, $\bigcap_{I \in \mathrm{Spec}R} I = \mathrm{rad}(0)$.

* 12. 据第 11 题, $\mathbf{Z}/(n)$ 的幂零根等于它的所有素理想的交. 类似于第 3 题的方法, 要求出

$$\mathrm{Spec}\mathbf{Z}/(n) = \{(p_1)/(n), (p_2)/(n), \cdots, (p_s)/(n)\}.$$

易证$(p_i)/(n)$与$(p_j)/(n)$互素，当$i \neq j$. 因此

$$\bigcap_{i=1}^{s}(p_i)/(n) = \prod_{i=1}^{s}(p_i)/(n) = (p_1p_2\cdots p_s)/(n).$$

习题 2.4

1. 注意$(m+ni)+(m-ni)=2m$，$(m+ni)(m-ni)=m^2+n^2$. 构造一个二次多项式$f(x)$，使它的两个根为$m \pm ni$.

2. 计算t^2, t^4，可看出t是哪个有理系数多项式的根.

3. 由于$f(x)=x^3-x+1$是$\mathbf{Q}[x]$中不可约多项式，因此$\mathbf{Q}[t]$中每个元素可唯一地表示成$c_0+c_1t+c_2t^2$的形式，由于$f(t)=0$，因此$t^3=t-1$. 从而可计算得

$$(5t^2+3t-1)(2t^2-2t+6)=32t^2+6t-2.$$

设$(3t^2-t+2)^{-1}=at^2+bt+c$，解$a,b,c$的一次方程组可求出$a, b, c$. 从而$(3t^2-t+2)^{-1}=-\frac{2}{7}t^2-\frac{1}{7}t+\frac{3}{7}$.

4. (1) 找出$GR(4^3)$的一个非平凡零因子，便知道$GR(4^3)$不是整环，从而(x^3+2x^2+x+3)不是$\mathbf{Z}_4[x]$的素理想.

(2) 可直接计算u^6, u^7，便知道u的阶.

*(3) 由于对任意$a,b \in \mathbf{Z}_4$，有$\sigma(a+b)=\sigma(a)+\sigma(b)$，$\sigma(ab)=\sigma(a)\sigma(b)$，且$\sigma(1)=1$，因此易证$\sigma$是$\mathbf{Z}_4[x]$到$\mathbf{Z}_2[x]$的一个同态. 显然$\sigma$是满射. 容易证明$\sigma$诱导了环$\mathbf{Z}_4[x]/f(x)$到$\mathbf{Z}_2[x]/(\bar{f}(x))$的一个满同态：$g(x)+(f(x)) \mapsto \bar{g}(x)+(\bar{f}(x))$.

*(4) 由于$\sigma(u)$的阶是u的阶的因子，从而由u的阶易求出α的阶.

*(5) 由于σ是同态，因此$\sigma(u^i)=\alpha^i$. 注意从α的阶可知道α是有限域$\mathbf{Z}_2[x]/(\bar{f}(x))$的乘法群的生成元.

*(6) 利用第(5)小题的结论，可证得$x_1=x_2$. 于是$2y_1=2y_2$，即$2(y_1-y_2)=0$. 从而$y_1-y_2=2\delta$，$\delta \in GR(4^3)$. 因此$\sigma(y_1-y_2)$

$=0$. 由此利用第(5)小题结论可得 $y_1=y_2$.

*(7) 利用第(6)小题结论可求出集合

$$\{x+2y \mid x, y \in T\}$$

的元素个数,与 $|GR(4^3)|$ 比较.

* 习题 2.5

*1. (1) 显然 $0 \in I$. 去证 I 对减法封闭,且有吸收性.

(2) 如果 $0 \overline{\in} S$,用反证法可证 $I \cap S = \emptyset$.

*2. 令 $T = R \times S$. 在 T 中规定一个二元关系 ~:

$$(a,s) \sim (a',s') \overset{\text{def}}{\Longleftrightarrow} as' - a's \in I.$$

去证 ~ 是等价关系,把商集 $T/\sim$ 记作 $S^{-1}R$,把 (a,s) 确定的等价类记成 $\frac{a}{s}$. 在 $S^{-1}R$ 中规定

$$\frac{a_1}{s_1}+\frac{a_2}{s_2}=\frac{a_1s_2+a_2s_1}{s_1s_2}, \qquad \frac{a_1}{s_1}\cdot\frac{a_2}{s_2}=\frac{a_1a_2}{s_1s_2},$$

去证上述定义不依赖于等价类的代表的选取.

易验证 $S^{-1}R$ 对于上述加法和乘法运算成为一个环. 零元素是 $\frac{0}{s}$,简记作 0. 单位元素是 $\frac{s}{s}$,简记作 $1'$,令

$$\sigma:\ R \longrightarrow S^{-1}R$$

$$a \longmapsto \frac{as}{s}.$$

易验证 σ 是一个环同态.

去证 $a \in \mathrm{Ker}\sigma \Longleftrightarrow a \in I$.

任取 $s \in S$. 易证 $\sigma(s) = \frac{ss'}{s'}$ 可逆,且它的逆为 $\frac{s'}{ss'}$. $S^{-1}R$ 的元素 $\frac{a}{s}$ 可以表示成 $\frac{a}{s} = \frac{as'}{ss'} = \frac{as'}{s'}\cdot\frac{s'}{ss'} = \sigma(a)\sigma(s)^{-1}$. 综上所述得,$S^{-1}R$ 是 R 关于 S 的分式环.

*3. $S = \mathbf{Z} - (p)$ 是由所有与 p 互素的整数组成.

易证 $I = (0)$, 从而 σ 是 $\mathbf{Z}$ 到 $S^{-1}\mathbf{Z}$ 的单同态. 于是可以把整数 a 与 $\sigma(a)$ 等同.

整数 a 在 $S^{-1}\mathbf{Z}$ 中可逆 $\Longleftrightarrow \sigma(a) = \frac{as}{s}$ 在 $S^{-1}\mathbf{Z}$ 中可逆. 由此推导下去, 可得 a 与 p 互素.

$S^{-1}\mathbf{Z}$ 的元素 x 可写成

$$x = \frac{a}{s} = \frac{rp^t}{s} = \frac{r}{s} \cdot \frac{p^t}{1} = \frac{r}{s}p^t\sigma(1)^{-1} = \frac{r}{s}p^t,$$

其中 $(a, p) = 1$; $t \in \mathbf{N}$. 由于 $s \in S$, 因此 $(s, p) = 1$.

$$x = \frac{r}{s}p^t \text{ 可逆} \Longleftrightarrow p^t \text{ 可逆} \Longleftrightarrow t = 0.$$

习题 2.6

1. (1) 先证 α 是单位 $\Longrightarrow N(\alpha) = 1$, 从而可求出 α. 由此可看出 α 是单位 $\Longleftrightarrow N(\alpha) = 1$, 并且可知道 $\mathbf{Z}[\sqrt{-5}]$ 的所有单位.

(2) 设 $N(\alpha) = 9$, 去证 α 的任一因子 β 为单位或者 β 与 α 相伴, 从而 α 是不可约元. 利用这个结论可立即得出, 3 和 $2 \pm \sqrt{-5}$ 都是不可约元.

(3) 由于 $9 = 3 \cdot 3$, 且 $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, 于是 $3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5})$. 假如 3 是素元, 则 $3 \mid (2 + \sqrt{-5})$ 或者 $3 \mid (2 - \sqrt{-5})$. 无论哪一种情况都可推出矛盾. 因此 3 不是素元. 类似地可证 $2 \pm \sqrt{-5}$ 都不是素元.

(4) 由于 3 是不可约元, 但是 3 不是素元, 因此 $\mathbf{Z}[\sqrt{-5}]$ 不是唯一因子分解整环. (或者由于 $9 = 3 \cdot 3$, $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ 是 9 到不可约元的两种不同的分解.)

*(5) 先证 3 与 $2 + \sqrt{-5}$ 的公因子只有 ± 1, 从而 3 与 $2 + \sqrt{-5}$ 有最大公因子 ± 1. 不妨设 $(3, 2 + \sqrt{-5}) = 1$.

假如9与$6+3\sqrt{-5}$的最大公因子存在，则

$$(9,6+3\sqrt{-5})=(3\cdot3,3(2+\sqrt{-5}))$$
$$=\pm3(3,2+\sqrt{-5})=\pm3.$$

不妨设$(9,6+3\sqrt{-5})=3$. 由于$(2+\sqrt{-5})|9$，$(2+\sqrt{-5})|(6+3\sqrt{-5})$. 因此$(2+\sqrt{-5})|3$，矛盾.

2. 假如$(2,x^2+1)=(g(x))$. 从$2\in(g(x))$可推出，$g(x)=\pm1$或±2. 不妨设$g(x)=1$或2. 从$g(x)\in(2,x^2+1)$可推出，$g(x)=2$. 于是$(2,x^2+1)=(2)$，由$x^2+1\in(2)$可推出矛盾.

*3. 令$\delta(\alpha)=N(\alpha)$，设$\alpha,\beta\in\mathbf{Z}[\sqrt{-1}]$，且$\beta\neq0$. 则$\alpha\beta^{-1}=u+v\mathrm{i}$，$u,v\in\mathbf{Q}$. 取整数$m,n$使得$|m-u|\leqslant\frac{1}{2}$，$|n-v|\leqslant\frac{1}{2}$. 令$\varepsilon=u-m$，$\eta=v-n$. 于是

$$\alpha=\beta[(m+\varepsilon)+(n+\eta)\mathrm{i}]=\beta q+r,$$

其中$q=m+n\mathrm{i}\in\mathbf{Z}[\mathrm{i}]$，$r=\beta(\varepsilon+\eta\mathrm{i})$. 易证$r\in\mathbf{Z}[\mathrm{i}]$. 去证$\delta(r)<\delta(\beta)$，因此$\mathbf{Z}[\sqrt{-1}]$是欧几里得整环.

4. 因为m没有平方因子，所以x^2-m在$\mathbf{Q}[x]$中不可约(用Eeisenstein判别法).

5. 去证R对减法、乘法封闭.

第三章　域扩张及其自同构

习题 3.1

1. $F(\alpha,\beta)=F(\alpha)(\beta)$. 由于$\beta$是$F$上代数元，从而$\beta$也是$F(\alpha)$上的代数元，因此$F(\alpha)(\beta)/F(\alpha)$是有限扩张，即$F(\alpha,\beta)/F(\alpha)$是有限扩张. 类似地，$F(\alpha)/F$是有限扩张. 因此$F(\alpha,\beta)/F$是有限扩张，从而它是代数扩张. 于是$F(\alpha,\beta)$中每个元素都是$F$上的代数元. 特别地，$\alpha+\beta,\alpha\beta,\alpha\beta^{-1}(\beta\neq0)$都是$F$上的代数元

2.(1) 易知 x^2-2 在 $\mathbf{Q}$ 上不可约,因此 $K=\mathbf{Q}[x]/(x^2-2)$ 是域,令 $\alpha=x+(x^2-2)$,则 $K=\mathbf{Q}(\alpha)$. 在 K 中,

$$x^2-2=(x-\alpha)(x+\alpha).$$

用反证法可证 x^2-3 在 $K[x]$ 中不可约,从而 $E=K[x]/(x^2-3)$ 是域. 令 $\beta=x+(x^2-3)$,则 $E=K(\beta)$. 在 E 中,

$$x^2-3=(x-\beta)(x+\beta).$$

于是在 E 中有

$$f(x)=(x-\alpha)(x+\alpha)(x-\beta)(x+\beta),$$

并且 $E=K(\beta)=\mathbf{Q}(\alpha)(\beta)=\mathbf{Q}(\alpha,\beta)=\mathbf{Q}(\alpha,-\alpha,\beta,-\beta)$. 因此 $E/\mathbf{Q}$ 是 $f(x)=(x^2-2)(x^2-3)$ 在 $\mathbf{Q}$ 上的一个分裂域.

$$[E:\mathbf{Q}]=[E:K][K:\mathbf{Q}]=2\times2=4.$$

(2) 易知,x^4-2 在 $\mathbf{Q}$ 上不可约,于是 $K=\mathbf{Q}[x]/(x^4-2)$ 是域,令 $\alpha=x+(x^4-2)$,则 $K=\mathbf{Q}(\alpha)$. 在 K 中

$$f(x)=x^4-2=(x-\alpha)(x+\alpha)(x^2+\alpha^2).$$

用反证法可证 $x^2+\alpha^2$ 在 $K[x]$ 中不可约,因此 $E=K[x]/(x^2+\alpha^2)$ 是域. 令 $\beta=x+(x^2+\alpha^2)$,则 $E=K(\beta)$. 在 E 中

$$f(x)=(x-\alpha)(x+\alpha)(x-\beta)(x+\beta),$$

并且 $E=K(\beta)=\mathbf{Q}(\alpha)(\beta)=\mathbf{Q}(\alpha,\beta)=\mathbf{Q}(\alpha,-\alpha,\beta,-\beta)$. 因此 $E/\mathbf{Q}$ 是 $f(x)$ 在 $\mathbf{Q}$ 上的一个分裂域,并且

$$[E:\mathbf{Q}]=[E:K][K:\mathbf{Q}]$$
$$=2\times4=8.$$

3.(1) 利用第二章 §3 的定理 7 和本节的定理 2,定理 3 可得出结论.

(2) 定义 $g(\alpha,\beta)=f(\alpha\beta)$, $\forall\,\alpha,\beta\in GF(q^m)$. 去证 $g(\alpha,\beta)$ 是域 $GF(q^l)$ 上线性空间 $GF(q^m)$ 的非退化对称双线性函数. 然后利用丘维声编著的《高等代数(下册)》第 322 页的第 5 题结论.

习题 3.2

1. (1) 类似于习题 3.1 第 2 题(2) 小题的方法可得,$E=\mathbf{Q}(\sqrt[3]{2},$

$\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)$，其中 $\omega=\frac{1}{2}(-1+\sqrt{3}i)$，$[E:\mathbf{Q}]=2\times3=6$.

(2) 由于 E 是无重根的 3 次多项式 $f(x)=x^3-2$ 在 $\mathbf{Q}$ 上的分裂域，因此 $E/\mathbf{Q}$ 是伽罗瓦扩张. 从而

$$|\mathrm{Gal}(E/\mathbf{Q})|=[E:\mathbf{Q}]=6.$$

又由于 $\mathrm{Gal}(E/\mathbf{Q})\cong G_f$，其中 G_f 是 $f(x)$ 在 $\mathbf{Q}$ 上的伽罗瓦群，它是在 $f(x)$ 的全部根组成的集合 $\Omega=\{\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$ 上的置换群，因此 $G_f\cong S_3$. 从而存在 $\tau,\sigma\in\mathrm{Gal}(E/\mathbf{Q})$，使得

$$\tau(\sqrt[3]{2})=\sqrt[3]{2},\quad \tau(\sqrt[3]{2}\omega)=\sqrt[3]{2}\omega^2,$$

$$\sigma(\sqrt[3]{2})=\sqrt[3]{2}\omega,\quad \sigma(\sqrt[3]{2}\omega)=\sqrt[3]{2}\omega^2.$$

于是可得出，$\mathrm{Gal}(E/\mathbf{Q})=\langle\tau,\sigma\rangle=\{1,\sigma,\sigma^2,\tau,\tau\sigma,\tau\sigma^2\}$

2. $\mathrm{Gal}(F_{2^m}/F_2)=\langle\sigma_2\rangle$，其中 $\sigma_2(\alpha)=\alpha^2$，$\forall\,\alpha\in F_{2^m}$.

习题 3.3

1. 用构造有限域 $GF(27)$ 的方法便可找出一个本原元素.

2. 直接用本节公式(8) 进行计算，这里 $p=2$.

3. (1) 直接验证. (2) 用反证法. 例如 $\chi_a=\chi_b$，则 $\forall\,x\in GF(q)$；有 $\chi_a(x)=\chi_b(x)$. 利用迹函数 Tr 是 $GF(q)$ 到 $GF(p)$ 的满射，可推出矛盾.

参考文献

[1] 聂灵沼,丁石孙.代数学引论(第二版).北京:高等教育出版社,2000

[2] 范德瓦尔登 B.L.代数学(I).丁石孙,曾肯成,郝钢新译.北京:科学出版社,1963

[3] Jacobson N. Basic Algebra (I). San Francisco: W. H. Freeman and Company,1974

[4] Armstrong M. A. Groups and Symmetry. New York: Springer-Verlag, 1988

[5] 柯斯特利金 A.И.代数学引论(下册).蓝以中,丘维声,张顺燕译.北京:高等教育出版社,1988

[6] КАРГАПОЛОВ М.И. МЕРЗЛЯКОВ Ю.И.群论基础.邓应生译.北京:高等教育出版社,1994

[7] Grove L. C. Algebra. New York: Academic Press,1983

[8] Kendig K. Elementrary Algebraic Geometry. New york: Springer-Verlag,1977

[9] Hecke E. Lectures on the Theory of Algebraic Numbers. New York: Springer-Verlag,1981

[10] Hungerford T.W.代数学.冯克勤译、聂灵沼校.长沙:湖南教育出版社,1985

[11] 李文林.数学史教程.北京:高等教育出版社,施普林格出版社,1999

索　引

（按名词所在页码出现的先后排序）

对称性(symmetry)　1
等边三角形(equilateral triangle)　1
保距变换(isometry)　2
群(group)　3
单位元素(identity element)　3
逆元素(inverse)　3
对称(性)群(symmetry group)　3
平面晶体群(plane crystallographic group)　4
贴墙纸群(wallpaper group)　4
空间晶体群(space crystallographic group)　5
爱尔朗根纲领(Erlangen Program)　6
环(ring)　8
交换环(commutative ring)　8
可逆元(invertible element)　8
单位(unit)　8
域(field)　8
代数结构(algebraic structures)　8
抽象代数(abstract algebra)　8
态射(morphism)　8
半群(semigroup)　11
幺半群(monoid)　11
阶(order)　12
循环群(cyclic group)　13
生成元(generator)　13
本原 n 次单位根(primitive nth root of unity)　13
关系(relations)　15
二面体群(dihedral group)　16
单位群(group of units)　16
一般线性群(General Linear Group)　16
特殊线性群(Special Linear Group)　16
正交群(Orthogonal Group)　17
特殊正交群(Special Orthogonal Group)　17
酉群(Unitary Group)　17
特殊酉群(Special Unitary Group)　17
矩阵群(Matrix Groups)　17
旋转群(rotation group)　17
全变换群(full transformation group)　17
置换(permutation)　17
n 元置换(permutation on n letters)

17
n 元对称群(symmetric group on n letters) 17
r - 轮换(r - cycle) 19
对换(trans position) 20
不相交(disjoint) 20
偶置换(even permutation) 23
奇置换(odd permutation) 23
交错群(alternating group) 23
正十二棱锥(right regular pyramid on a twelve sided base) 23
正六边形(regular hexagon) 23
正五边形(regular pentagon) 23
正四面体(regular tetrahedron) 24
正方体(cube) 24
子群(subgroup) 25
置换群(group of permutations) 26
变换群(transformation group) 26
平凡子群(trivial subgroups) 26
非平凡的(non - trivial) 26
由 S 生成的子群(subgroup generated by S) 27
⟨S⟩的生成元集(set of generators for ⟨S⟩) 27
有限生成的群(finitely generated group) 27
特征为 0(characteristic 0) 29
特征为 p(characteristic p) 29
左陪集(left coset) 32
左商集(left quotient set) 32
右陪集(right coset) 32
右商集(right quotient set) 33
基数(cardinal number) 33
指数(index) 33
费马小定理(Fermat's Little Theorem) 34
高斯整数群(group of Gaussian intergers) 38
同构的(isomorphic) 40
同构(isomorphism) 41
直积(direct product) 44
直和(direct sum) 44
内直积(internal direct product) 48
内直和(internal direct sum) 48
同态(homomorphism) 51
满同态(epimorphism) 51
单同态(monomorphism) 51
嵌入(embedding) 51
正规子群(normal subgroup) 54
共轭子群(conjugate subgroup) 54
商集(quotient set) 56
商群(quotient group) 56
自然同态(natural homomorphism) 57
标准同态(canonical homomorphism) 57
单群(simple group) 60
换位子(commutator) 61
换位子群(commutator subgroup) 61
导群(derived group) 61
导群列(derived groups series) 63
可解群(solvable group) 63

半直积(semidirect product) 66
作用(action) 67
忠实的(faithful) 68
左平移(left translation) 69
共轭作用(conjugation action) 70
中心(centre) 70
自同构(automorphism) 71
内自同构(inner automorphism) 71
自同构群(automorphism group) 71
轨道(orbit) 72
传递的(transitive) 72
齐性空间(homogeneous space) 72
共轭类(conjugacy class) 73
类方程(class equation) 73
共轭元素(conjugacy elements) 73
稳定子(stabilizer) 73
中心化子(centralizer) 73
特征子群(characteristic subgroup) 79
型(type) 80
分拆(partition) 80
正规化子(normalizer) 80
等价的(equivalent) 81
乘积作用(product action) 82
四元数(quaternion) 88
四元数体(quaternion field) 89
四元数群(quaternion group) 89
初等因子(elementary divisors) 93
极小生成元集(minimal set of generators) 93
初等 abel p－群(elementary abelian p－group) 100
秩(rank) 100
自由 abel 群(free abelian group) 100
自由生成元集(free set of generators) 102
自由群(free group) 102
字(word) 102
既约的(reduced) 102
空字(empty word) 103
由 X 生成的自由群(free group generated by X) 103
一组定义关系(a set of defining relations) 106
表现(presentation) 107
有限表现的(finitely presented) 107
组合群论(Combinatorial Group Theory) 107
辫子(braid) 108
辫指数(braid intex) 108
辫群(braid group) 110
初等辫子(elementary braids) 110
自由积(free product) 113
左零因子(left zero divisor) 114
右零因子(right zero divisor) 114
整环(Commutative domain) 114
除环(division ring) 114
子环(subring) 115
零点(zero point) 117
超曲面(hypersurface) 117
仿射超曲面(affine hypersurface) 117

平面曲线(plane curve) 117
曲面(surface) 117
代数簇(algebraic variety) 117
仿射代数簇(affine algebraic variety) 117
代数几何(algebraic geometry) 117
理想(ideal) 118
左理想(left ideal) 118
右理想(right ideal) 118
单环(simple ring) 118
由 S 生成的理想(ideal generated by S) 119
主理想(principal ideal) 119
互素(coprime) 121
根(radical) 122
幂零元(nilpotent element) 122
幂零根(nilradical) 122
商环(quotient ring) 123
剩余类(residue class) 123
a,b 模 I 同余(a is congruent to b modulo I) 129
素理想(prime ideal) 135
谱(spectrum) 135
代数封闭域(algebraically closed field) 136
极大理想(maximal ideal) 139
扩环(extension ring) 140
极小多项式(minimal polynomial) 145
代数数(algebraic number) 146
超越数(transcendental number) 146
代数整数(algebraic integer) 146
代数数域(algebraic number field) 146
分圆域(cyclotomic field) 146
在 R 上是超越的(transcendental over R) 147
在 R 上是代数的(algebraic over R) 147
基本不可约的(basic irreducible) 148
代数无关的(algebraically independent) 150
代数相关的(algebraically dependent) 150
有理函数域(rational function field) 152
分式域(field of fractions) 152
乘性子集(multiplicative subset) 155
分式环(ring of fractions) 156
因子(factor 或 divisor) 156
倍数(multiple) 156
相伴(associates) 157
真因子(proper factor) 157
平凡因子(trivial factors) 157
不可约的(irreducible) 157
可约的(reducible) 157
素元(prime element) 157
公因子(common divisor) 158
最大公因子(greatest common divisor) 158
唯一因子分解整环(unique factorization domain) 159

高斯整环(Gaussian domain)　159
因子链条件(divisor chain condition)　159
主理想整环(principal ideal domain)　162
欧几里得整环(Euclidean domain)　163
本原多项式(primitive polynomial)　164
理想的升链条件(asending chain condition for ideals)　166
诺特环(Noether ring)　167
希尔伯特基定理(Hilbert Basis Theorem)　167
范数(norm)　169
代数整数环(ring of algebraic integers)　170
子域(subfield)　171
扩域(extension field)　171
域扩张(field extension)　171
中间域(intermediate field)　171
素域(prime field)　172
单扩张(simple extension)　172
K在F上的次数(degree of K over F)　173
有限扩张(finite extension)　173
基(basis)　173
代数扩张(algebraic extension)　173
单代数扩张(simple algebraic extension)　174
单超越扩张(simple transcendental extension)　174
分裂域(splitting field)　176
伽罗瓦域(Galois fields)　182
正规扩张(normal extension)　182
可分的(separable)　184
可分扩张(separable extension)　184
不动域(fixed field)　188
伽罗瓦群(Galois group)　190
伽罗瓦扩张(Galois extension)　190
Frobenius自同构(Frobenius automorphism)　194
本原元素(primitive element)　195
迹(trace)　196

高斯整环(Gaussian domain)　159
因子链条件(divisor chain condition)　159
主理想整环(principal ideal domain)　162
欧几里得整环(Euclidean domain)　163
本原多项式(primitive polynomial)　164
理想的升链条件(asending chain condition for ideals)　166
诺特环(Noether ring)　167
希尔伯特基定理(Hilbert Basis Theorem)　167
范数(norm)　169
代数整数环(ring of algebraic integers)　170
子域(subfield)　171
扩域(extension field)　171
域扩张(field extension)　171
中间域(intermediate field)　171
素域(prime field)　172
单扩张(simple extension)　172
K 在 F 上的次数(degree of K over F)　173
有限扩张(finite extension)　173
基(basis)　173
代数扩张(algebraic extension)　173
单代数扩张(simple algebraic extension)　174
单超越扩张(simple transcendental extension)　174
分裂域(splitting field)　176
伽罗瓦域(Galois fields)　182
正规扩张(normal extension)　182
可分的(separable)　184
可分扩张(separable extension)　184
不动域(fixed field)　188
伽罗瓦群(Galois group)　190
伽罗瓦扩张(Galois extension)　190
Frobenius 自同构(Frobenius automorphism)　194
本原元素(primitive element)　195
迹(trace)　196